INFORMATION SECURITY & PRIVACY NEWS

A Publication of the Information Security Committee
ABA Section of Science & Technology Law

SUMMER 2014 VOLUME 5 ISSUE 3

Establishing a Strategic Framework for Litigation and Risk Mitigation

By Donna Chesteen and Scott Crespo

2013 was an active year in the field of information security. Four of the top ten data breaches of all time occurred in 2013, and three of these incidents involved American corporations: Adobe Systems, Inc. took the top spot with 152 Million records exposed due to a malicious attack; Target Brands, Inc. ranked at number 5 with the exposure of 110 Million records; and Pinterest comes in 10th place with the exposure of 70 Million records. For the foreseeable future, it does not appear that the scope and frequency of data breaches will decrease, even as budgets to combat the phenomenon are rising rapidly. Already this year, we've seen another record-breaking *Read more*

Does Personal Privacy Matter? Developments in EU & US Data Retention Law

By Camille A. Stewart

In the wake of classified data leaked by former National Security Agency (NSA) contractor Edward Snowden, privacy and surveillance are under increased international scrutiny. It is no surprise that the European Union ("EU") and the United States ("U.S.") have taken this opportunity to reevaluate their data retention laws. On April 8, 2014, the EU's highest court struck down the controversial directive that required telecommunications and mobile phone companies to retain users' private data records for up to two years. This revelation will not only have an effect on data retention in the European Union, but also will be a factor as the U.S. considers *Read more*

THE WEAKEST LINK: Why and How We Must Embed Security Controls into Business Processes Now

By Betty K. Steele and Frederick Scholl

The Information and cyber security breaches often occur because organizations do not properly understand or manage risk associated with their vendors, service providers and partners. In many instances, organizations and their vendors, service providers and partners have security controls that have not been operationalized or do not follow their own security policies, despite often having dozens or more security professionals on staff. Such was the case in the recent Target breach, where, as has been reported, hackers used the credentials of an HVAC vendor to get into Target's network and grab customer card information. *Read more*

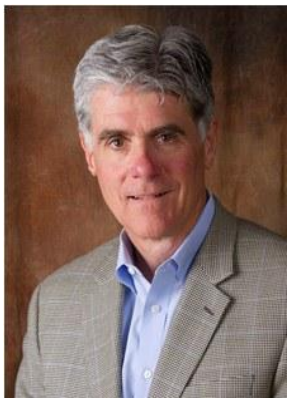
2014 (2Q) Information Law Updates: Cases, Statutes, and Standards

By Thomas Shaw

In the second quarter of 2014 and the end of the first quarter, there have been many developments in U.S. and international information security, privacy, and cloud computing statutes, cases and standards. This includes international and U.S. state and federal laws and regulations that have been passed or are coming into force. It also involves civil and criminal cases and enforcement actions brought by regulators. And it encompasses the new standards, guidelines and legal ethics opinions in this area, while not attempting to track legislation that has not yet been passed. To briefly summarize the major developments in this area of law and practice, each significant development is presented with a brief analysis after it. *Read more*

THE WEAKEST LINK: Why and How We Must Embed Security Controls into Business Processes Now

By Betty K. Steele and Frederick Scholl

Information and cyber security breaches often occur because organizations do not properly understand or manage risk associated with their vendors, service providers and partners. In many instances, organizations and their vendors, service providers and partners have security controls that have not been operationalized or do not follow their own security policies, despite often having dozens or more security professionals on staff. Such was the case in the recent Target breach, where, as has been reported, hackers used the credentials of an HVAC vendor to get into Target's network and grab customer card information.

In another instance, during a crash investigation, it was widely reported that Malaysia Airlines, a carrier with flights to Los Angeles, apparently did not check passports against an international lost/stolen passport database, potentially introducing threat agents, holders of lost or stolen passports, by allowing them to enter the U.S. or another country. Similarly, Santa Barbara, California police failed to check a readily available state database of gun purchases prior to making a welfare check on a disturbed college student at the behest of his concerned parents.[1] Six university students and the shooter died in the resulting incident. More disturbing from a sheer scope and potential impact perspective has been the 2013 electric substation attack in the San Jose, California area by gunmen, which nearly took out power in that region.

All four of the realized or potential breaches noted in the preceding paragraph highlight the links between users and organizations with their vendors, service providers and partners. Both the Target breach, in which a vulnerability through a service provider was exploited by a threat agent, and the reported Malaysia Airlines vulnerability that in this instance was not exploited by a threat agent, highlight how a seemingly innocuous service provider, an HVAC company, and an anything but innocuous foreign airline, Malaysia Airlines, can compromise personally identifiable information (PII) in the former case and critical infrastructure (CI) in the latter case. Failure by police to check a readily available gun purchases' database and confiscate those guns may have contributed to an incident that could potentially have been averted. Finally, the 2013 attack on the electric substation was a clear breach of a vulnerability by a most dangerous threat agent – a threat agent who might strike again.

[1] "Calif. Police didn't check database before rampage", Washington Post, May 30, 2014. See also The Sacramento Bee, June 12, 2014.

While there are numerous international, U.S. and state laws, regulations, and mandated contractual obligations relating to protection of PII and CI that have been in place for years, it is clear that many organizations and their vendors, service providers and partners are still falling down on the job. The good news is that the security methodology developed to protect PII and CI, by and large, applies across industry sectors and geographic boundaries. The challenge is that this methodology has not been effectively applied across these sectors. We have the tools and knowledge, but many times we are using neither. As information—data and software--has become embedded into the devices and systems we use every day, we face an information (and cyber security) crisis similar to the late 1970's manufacturing quality crisis in the U.S. We believe that some of the same solutions that worked then will work now.

In this article we will make the case for the importance of embedding security into business processes. We feel that many security breaches could be averted and quality of products and services improved if that were so. With that in mind, we have structured this article as follows: the first section provides background on and motivations for implementing this security quality transformation now; the second section contains a short review of an approach to be taken for compliance with information and critical infrastructure security laws, regulations and common contractual requirements[2]; and, finally, in the third section, we will provide an approach and best practices that help organizations implement security into business processes, based on previous experience with the manufacturing quality crisis.

1. Background and motivation

In the beginning information security was simple. The focus of the information security effort was a physically imposing box–the mainframe computer and its accompanying processes – used to accomplish multitudinous tasks such as bulk data processing, statistical analysis, transaction processing, and the like. Both physical and logical connectivity were limited and often discrete. The Internet as we know it was but a gleam in the eye. Security was blunt and direct – locks, alarms, information classifications, employees with clearances, and the like.

As connectivity complexity and use of the Internet increased, information security management as a discipline became more visible within the organization and security professionals started to look at the criticality of the information that could be compromised. Prompted by consumers who did not appreciate having their PII stolen by the "bad guys", with no recourse against the organizations in which the breaches occurred, laws and regulations started to spring up.

[2] This section is short not because it is not important, but rather to go through security laws, regulations, contractual requirements, frameworks, and standards in detail is not only well beyond the scope of this article, but also the topic of many scholarly books and articles. This article is about how quality can help drive security, the effect of which should be to help organizations better comply with those laws, regulations and contractual provisions, as well as improve business performance.

Despite these activities, we now are in a place where security breaches are common and, indeed, our critical infrastructure is at risk. What went wrong? The biggest problem we see is that effective security controls did not get implemented within the business. Yes, security is bolted on in many firms, but this approach has not worked effectively. For an information security program to work, it must be embedded within the business processes. There are three drivers behind doing this now: time, business benefits and visibility. If security professionals get behind this strategy, then we can hope to see a new generation of effective security programs. None of our ideas are new here, but we feel they are worth restating and revisiting.

Change is the universal enemy of security. In the days of EDP[3] (Electronic Data Processing) security, it was feasible to add security well after systems were developed. The lifecycle of systems was measured in years and the threat landscape changed even more slowly. If a built system was found to need additional security controls, they could be retrofitted. The original IBM 360 was introduced in 1965; the RACF[4] (Remote Access Control Facility) security system followed 11 years later in 1976. Today systems are introduced and changed at a continuous pace of innovation. We are well into or past the accelerated change scenarios described by Toffler. [5] However, budget cycles are still 1-3 years. Any new security requirement that is not included in the business system and process development cycle will be delayed by at least this length of time. After business unit leaders negotiate funding with their CFO's and CEO's for 1-3 years, they will not listen to the fears of the security professionals who may want to further delay their projects.

Like it or not, business executives will rarely approve security programs without a defined business benefit. Any security program should seek to demonstrate such benefits. Research work has attempted to quantify these benefits. Phelps and Milne[6] were one of the first groups to analyze the connections between high performing organizations and mature security controls. In their work, positive correlations were shown, but their research analyzed only the benefits to the operations of the IT department itself. More recently, IBM has published its Global C-Suite study[7] of 1656 CIOs from 62 countries. One goal of the work was to understand the correlation between enterprise business performance (revenue growth and profitability) and CIO strategies. The study reported that 60% of the "outperformers" were making more effort to improve their resources for managing risk, whereas only 39% of the underperformers were doing so.

---

[3] Stepping Through the InfoSec Program, Jennifer Bayuk, 2007.
[4] Mainframe Basics for Security Professionals, Ori Pomerantz, et al, 2008.
[5] Future Shock, Alvin Toffler, 1970.
[6] "Leveraging IT Controls to Improve IT Operating Performance", Daniel Phelps and Kurt Milne, 2008.
[7] "The Customer-activated Enterprise: Insights from the Global C-suite Study", IBM Institute for Business Value, October, 2013.

Other trends indicate that now is the right time to push security out of the CIO/IT tower. For one thing, the CIO is being pushed out of the IT tower. More and more "IT" initiatives are being initiated and run from within the business units. Author and executive recruiter Martha Heller[8] recommends that CIO's reorganize from a traditional plan, deliver, run model to a structure of mini-CIOs each accountable for IT strategy and delivery to one major business unit. The security function should follow this recommendation.

Some good news is that the security role is now starting to be taken more seriously at the top levels. Reuters reports[9] that more CIO's and CISO's are being sought after for board positions on public companies. According to Reuters, this trend is in support of the view that cybersecurity is more a business issue than a compliance issue and that boards need to make sure that security is designed into products, not just bolted on. A confluence of trends, including major breaches and security news reports, is combining to create extra visibility for security at the board and executive level thus making it possible for security to become an ongoing part of business processes.

2. Applicable laws, regulations and contractual requirements

Notwithstanding the trends noted above, a principal driver of security policies, plans and related contractual requirements is that organizations are arguably required by law to have them in place and to implement them. Every "sane" and "cognizant" organization has information and/or processes it wants to protect, even if it does not itself have any PII or CI. At the very least, the organization uses electricity and water, both of which are dependent upon technology systems to operate. The destruction of such systems, through low tech but effective methods such as attacking gunmen, as noted in the discussion of the San Jose substation above, can take down cities', states' and countries' electric grids. On a more mundane level, any organization that has an informational web site, at the very least, wants the information on the site to be accurate and untampered with. Smaller companies often cannot withstand a significant breach and even large companies, like Target, can sustain major financial and career ending losses. Consumer lawsuits, government enforcement actions and shareholder driven SEC investigations can certainly drain company coffers.

Laws and regulations to protect PII, CI and related processes are summarized in the recent ABA Information Security and Privacy Handbook and we commend that book to anyone wanting a thorough review of the subject.[10] Since there have been and continue to be so many breaches impacting PII, CI, trade secrets, business processes, and the like and so many different types of PII that are the subject of international, federal, state, and, in some cases, local laws, regulations and other requirements, many organizations approach compliance by using the international standard ISO/IEC 27001 2013 Information technology -- Security techniques -- Information security management systems –

[8] The CIO Paradox, Martha Heller, 2013.
[9] "US Companies seek cyber experts for top jobs, board seats", Reuters, May 29, 2014.
[10] Information Security and Privacy, Thomas J. Shaw, Editor, 2011.

Requirements ("ISO/IEC 27001"). That standard addresses security comprehensively and includes sections on both supplier relationships and compliance. With regard to compliance with legal requirements, it is recommended in ISO/IEC 27001 that organizations (i) identify applicable security and privacy legislation and contractual obligations that protect health, financial, children's, employee, credit, and other information and resulting contractual[11] and related obligations; (ii) enforce third party intellectual property rights relating to technology and software; (iii) protect organizational records, particularly electronic records, consistent with laws, regulations, and the like; (iv) protect data and the privacy of PII; and (v) ensure regulations regarding cryptographic controls are met.

On the CI front, there have been recent and significant developments. Under the Computer Security Act of 1987, the National Institute for Standards and Technology ("NIST") was given the responsibility for developing security standards for Federal Information Systems. Executive Order 13636 (2013) gave additional responsibility to NIST for developing a risk based framework for all of the nation's critical infrastructure. The result was the "Framework for Improving Critical Infrastructure Cybersecurity" ("Framework Core") (2014).

The Framework Core is a risk-based approach to managing cybersecurity risk that at present is voluntary. The basis of the Framework is: (1) using business drivers to guide what is important to the organization for cybersecurity purposes; and (2) incorporating cybersecurity risks into an organization's enterprise risk management. The Framework Core, which provides a set of activities to achieve specific cybersecurity outcomes, and guidance to achieve these outcomes, also contains risk management maturity tiers. In addition, a common flow of information and decisions at the executive, business/process and implementation/operations levels are expected. The Framework is cross-referenced to other standards, best practices, and frameworks, including ISO/IEC 27001, NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Rev. 4, and COBIT 5 "A Business Framework for the Governance and Management of Enterprise IT". It covers and provides sector specific resources for the following sectors: chemical, energy, healthcare, commercial facilities, communications, critical manufacturing, dams, defense, emergency services, financial services, food and agriculture, government facilities, IT, nuclear reactors, transportation, and water and wastewater.

3. An approach to implementing security in business processes

So, with all the legal, regulatory, contractual and vendor, supplier and partner complexity, keeping PII, CI and business processes safe and secure is a moving target and a real challenge. Lack of understanding of risk, management of risk, different threat agents, vulnerabilities, and how to manage vendors, suppliers and partners, even seemingly innocuous ones such as HVAC vendors is overwhelming – an "information quality problem". Similarly, in the 1970's the U.S. faced a

[11] The Payment Card Industry Data Security Standard is a requirement placed on merchants and service providers that store, process or transmit cardholder data to have security in place.

manufacturing quality problem, especially in the automotive area. (As used here, "quality" is defined as "conformance to requirements"[12].) Concern then centered on quality advances made by the Japanese automotive industry in particular. The U.S. Big Three automobile manufacturers, GM, Ford and Chrysler, had failed to heed the call about product quality, which was evident to middle managers but not to the C-suite. By the time the C-suite saw the light, considerable market share had been ceded to foreign automakers. Japanese industrialists, in order to jump start their post WW II economy, had heeded the call of quality control and quality management giant William Edwards Deming, and the results yielded greatly improved quality and greatly increased productivity.

Subsequently, the U.S. adopted some of the same quality methods, such as lean, six sigma, and TQM. While initially these quality methods were viewed in a strict manufacturing context, subsequently the quality movement extended as an enabler for improved business performance for all organizations. This culminated in programs like the Baldridge Criteria[13] created in the late 1980s. In addition, the automotive industry brought the supply chain into its quality orbit. C-suite executives can take a page from the manufacturing crisis book when addressing today's information and CI security crisis and use some of the same methods to improve their security programs. Many in information security today argue that attractive features and good security are mutually exclusive. One need only look at the quality and features built in to the family car to see that this concept is not correct.

We believe that effective information security can be implemented using many of the methods used to solve other quality problems. And while the "devil is in the details" we believe that making the connection between information security requirements (and processes) and quality is quite doable and important. Organizations, particularly those steeped in quality methodologies, should be able to invoke all of their experience in successfully implementing quality programs to achieving information security results by merging their security controls and initiatives into business processes.

Most people still think of moats or firewalls when they think of information security. This paradigm is in fact entrenched in the minds of many security practitioners and managers. However, the most common security control frameworks already discussed have only a small subset of controls devoted to perimeter security or control. Instead, these frameworks are better thought of as assuring the quality of the information being managed. What is quality? According to Crosby it is: "conformance to requirements". Therefore, what we call "information security" today can be well understood as "information quality" and by using the concepts from traditional quality management we can make more effective progress in securing our increasing volume of information.

[12] Quality is Free, Philip Crosby, 1979.
[13] The Executive Guide to Understanding and Implementing the Baldridge Criteria, Denis Leonard, Mac McGuire, 2007

Traditional information security is defined by the CIA triad: confidentiality (C), integrity (I) and availability (A). These control objectives apply to the business processes being supported and could include management processes, operational processes and supporting processes. Applying the CIA triad would mean the objective of the security program would be to, for example, prevent the leakage of HR data (C), make sure manufacturing processes run reliably (A) and prevent data changes in accounting records (I). These objectives can be understood as assuring that the specific business process meets the requirements of the process owner, who might be the HR manager, the manufacturing manager, or the head of accounting, in the examples. For purposes of this discussion, theft of confidential information (usually copying) occurs because a business process does not have suitable controls to protect its operation. In the quality paradigm, it did not meet the requirements of the owner. In the case of Target, the business process was sales and the breach severely disrupted that process.

Previous authors have noted the connection between security and information quality. For example ITIL v1 states: "The degree to which the business processes depend on the information supply has to be specified in quality requirements for the information supply. In that sense, information security must therefore form an integral part of an organization's overall quality management and quality assurance procedures"[14]. Owen[15] describes how the Johnson Space Center used TQM methods to both build security into systems development processes and save money at the same time. Security pioneer Gene Kim stated back in 2008: "In order to remain sustainable and viable in the organization, information security must transition from being merely a management edict to being an integral part of daily business operations."[16]

The big benefit of this way of thinking is that it allows us to use all the management and technical machinery associated with traditional quality management, that is, from thought leaders in traditional quality management i such as Deming, Crosby and Joseph Juran[17]. Such quality management techniques have already been accepted by business leaders. The security control frameworks cited provide controls to enable organizations to implement an information quality program. Techniques, from traditional quality management systems, that we can adopt to help implement and then monitor these control frameworks are discussed below. By using existing quality paradigms and frameworks, we can avoid obstacles in actually implementing an effective security program. Many organizations talk about security, but few actually make it happen on a sustainable basis. That is what we hope to help enable.

[14] Security Management, ITIL, 1999.
[15] "Security Management: Using the Quality Approach", Richard Owen, 15th National Computer Security Conference, 1992
[16] Visible Ops Security, Gene Kim, Paul Love, George Spafford, 2008.
[17] Quality Planning and Analysis, Joseph Juran and Frank Gryna, 1970.

As an example, we will look at the COSO framework[18] and illustrate how traditional quality management would help implement the COSO control objectives. We use COSO simply as an example; there is no shortage of good security control frameworks as we mentioned previously. The point of this section is to shed light on methods for *successfully implementing* any of these frameworks.

COSO Objective	**Traditional Quality Implementation**
Control Environment	Active participation of C-level
Risk Assessment	Conformance to requirements; PDCA
Control Activities	Embedded in the workforce
Information and Communication	Good understanding of people's motivations
Monitoring	Management visibility of analytical results

- *Control Environment*. In COSO parlance, the "control environment" is the tone at the top. Many security programs trudge forward without the right tone the top. In fact, it is an art to achieve this tone. Experiencing a breach may establish a security crisis tone, but that is not the tone needed for long-term continuous improvement. Quality professionals have worked long and hard to establish their approaches to getting management buy in[19]. Successful quality outcomes in manufacturing have been based on management participation, not just support. In a well-known case study, Paul O'Neill turned Alcoa around[20] by focusing on corporate safety processes. In an information-centric company the same type of outcome might be anticipated by a focus on information security.

- *Risk Assessment.* The security methodology PDCA originated with Deming's work on quality. Manufacturing quality developed the concept of QFD (Quality Function Deployment) in the 1960's. This emphasized the introduction of quality into the design phase of the product. Adherence to specifications and frameworks has been emphasized by Donn Parker[21]. Many security professionals stress the need for threat modeling to analyze organizations' specific threat actors. The fact is that most breaches originate in failures to implement well understood security controls. We yet believe that risk analysis has its place in security, at a minimum to prioritize remediation activities.

- *Control Activities*. Security professionals commonly divide the organization's population into "security professionals" and "users". The job of the former is to implement controls to protect the users, who are either making mistakes or sabotaging systems. This paradigm actually sabotages the security program itself. In contrast, Crosby states that: "quality is much too important to be left to professionals". Juran's concept of quality control was based on self-control: "when work is

[18] www.coso.org
[19] The Art of Getting Your Own Sweet Way, Philip Crosby, 1981.
[20] "Can Good Habits Really Mean Big $$ for Business", Maureen Mackey, www.thefiscaltimes.com, April, 2012.
[21] "Making the Case for Replacing Risk-Based Security", Donn Parker, ISSA Journal.

organized in a way which enables a person to have full mastery over the attainment of planned results, that person is said to be in a state of self-control and can therefore be held responsible for the results." This concept applies in today's information world, where there are not clear boundaries between outsiders and insiders, hackers and careless or deceitful employees.

- *Information and Communication.* Both quality and security are fundamentally a people issue. And people do not act without information that is well communicated. Crosby offers more good advice on this topic: "…some people are just plain not interested in learning anything that will make them have to change. Therefore quality education needs to be visibly oriented toward the product, the service and the customer". Today's "security awareness" training needs to be upgraded significantly, by focusing on the business as one step.

- *Monitoring.* It is the stepchild of information security, often added in at the end of security control development, and then inadequately staffed. Security "penetration testers" are sought after by clients, however, their reports are really the equivalent of "outgoing quality inspection" in a manufacturing environment. Any outbound quality test will result in the most costly remediation task. Manufactured quality lives and dies on the concept of "zero defects": do it right the first time. Zero defects is achieved by strict incoming product quality monitoring, in-process monitoring and outgoing inspection. This monitoring makes use of statistical control charts and enables detection of out of control processes and planned process improvement. Security thought leaders like Jones[22] have already incorporated these ideas in to their risk management strategy.

Conclusions

"There are no technical solutions to management problems, but there are management solutions to technical problems"[23]. This concept is well accepted by security professionals. The weak link is to define and execute 'management solutions' to mitigate information security risks whether they reside within the organization or with a vendor, service provider or partner. We have argued that this solution must include embedding security into business processes. Visibility of cybersecurity risks is at an all-time high. In Jamie Dimon's April, 2014 Letter to Shareholders, he states: "…cyberattacks are growing every day in strength and velocity across the globe. It is going to be a continual and likely never-ending battle to stay ahead of it…"[24]. It is up to security professionals to take advantage of this type of visibility. We suggest that following the methodology and successes of the enterprise quality movement will be a fruitful path to continuous, adaptable and sustainable security controls, embedded in business processes.

[22] "A Practical Approach to Risk Management", Bruce Jones, RSA 2011.
[23] RFC 4949, Courtney's Third Law
[24] JP Morgan Chase, Letter to Shareholders, April 9, 2014.

***Betty K. Steele, Esq**., CISSP, ITIL, leverages her experience and expertise in law, technology, quality, process improvement, and business in order to help organizations to meet their ethical, governance and compliance responsibilities, their legal and regulatory requirements, and their strategic, tactical and operations objectives from an IT perspective. She received her J.D. from Vanderbilt University Law School, where she was a member of the Vanderbilt Law Review, and her undergraduate degree at Brown University. She is president of the Society for Information Management Nashville Chapter.*

***Frederick Scholl** is Visiting Professor of Information Security at Lipscomb University in Nashville, TN. He teaches graduate courses on Legal, Technical and Compliance Concerns, Secure IT Communications & Operations, Business Continuity and Disaster Recovery, and Risk Assessment & Mitigation Planning. He is also President of Monarch Information Networks, LLC and provides information security risk management services and expert witness services. Fred has a PhD in Electrical Engineering from Cornell and CISSP, CISM, ITIL, CHP and PCIP certifications.*