

DIGITAL TRUST FOR LIFE PROJECT REPORT



July 2009

ACLI
Financial Security. For Life.

CSC

**USING DIGITAL TRUST TO
CREATE NEW ENTERPRISE
VALUE FOR THE LIFE AND
ANNUITY INDUSTRY**



TABLE OF CONTENTS

Executive Summary	2
Trust at the Core	2
Intersecting Digital Realities	2
Questions Asked	3
... and Answered.....	3
Digital Trust Potential	4
Pursuing Enterprise Value with Digital Trust	4
Now, More Than Ever	5
Putting “Life” into Digital Trust	6
The Beginning.....	6
Life and Annuity “Value Objectives”	6
Payoffs	7
Traditional Information Risk Management.....	7
Digital Trust Dividends	8
Digital Trust Deficits	9
Compliance Penalty Potential in the Life and Annuity Industry	10
Doing “Digital Trust for Life”	12
The Study Plan.....	12
Industry Interviews and Conversations	12
Reporting	13
Part 1 — Digital Trust Analysis.....	14
Customer Service and Distribution Management	14
Organic Growth and Competitive Advantage	17
Digital Trust in Evidence?.....	19
Still the “Gatekeeper” Model	19
Digital Trust Promotes Security Value Identification and Capture	20
Digital Trust Analysis Results	22
Missed Steps.....	22
Payoff Potential Remains.....	23
Part 2 — Digital Trust Projection	24
Initial Business-Impact Areas	24
“What If” Scenarios for Digital Trust Technology Projections	25
Conclusions and Recommendations	28
Study Observations and Conclusions.....	28
Recommendations	29
Action 1: Alter the IT Risk Governance Model to Support Digital Trust.....	30
Action 2: Bring Digital Trust to Current Systems	31
Becoming a Digital Trust Enterprise.....	31
Appendix A CSC Digital Trust Research Program Overview (Extracted From Volume 8, Epilogue and Strategic Roadmap).....	33
Shake Hands with the Digital Enterprise	33
Strategic Conclusions.....	34
What Now?.....	34
Unexamined Realities	35
Acknowledgements	39
Special Thanks.....	40



EXECUTIVE SUMMARY

Trust at the Core

Perhaps no other industry has “trust” more at the core of its business operations than the insurance industry. Potential clients must trust the integrity and fair representation of agents and producers. Consumers must trust in the long-term financial stability and resources of the insurance provider. And policyholders must trust that their sensitive personal information, given in fulfillment of their own trust obligation, will not be abused by the insurance company itself. For centuries, the handshake between company representatives and clients has always stood for “trust.”

Intersecting Digital Realities

That trust, so carefully nurtured in the real world by insurance industry representatives, must now become evident in the digital world, as well. Today, trust requirements for the digital enterprise of the insurance industry are often introduced or derived through new state and federal statutes, regulatory directives and standards of performance. Compliance with such mandates has become a never-ending requirement for the industry, with costs already estimated to consume from \$600 million to over \$6 billion annually.¹

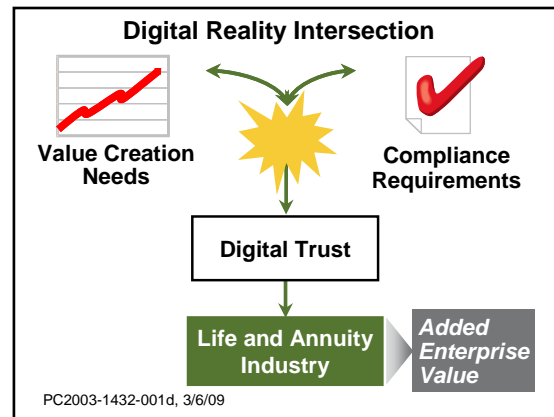
This is, by now, a familiar reality for the insurance industry:
There will always be new and more compliance requirements for the digital enterprise.

The pursuit of that reality has meant investment after investment in compliance efforts and technology for each digital system and process introduced or supported by the digital enterprise. As early as 2004, that effort was estimated to take 20 percent of new IT project expenditures.²

With no relief in sight, is this “just the cost of doing business”? Conventional wisdom suggests that such expenses simply prevent existing enterprise value from being destroyed. Is there no better way for insurance carriers, who continue to invest large sums in compliance and security for the digital enterprise, to reap enterprise value from that investment?

The answer to those questions comes from a *new reality* for all digital enterprises, including those supporting the insurance industry. This is the reality of **Digital Trust**:
Creating new enterprise value with security services and technologies rather than only incremental improvement in the protection of value that already exists.

A recent 18-month study by CSC³ has given definition to Digital Trust and revealed the nature of its workings. The research showed that conventional wisdom often overlooks the reality of value creation with security services and technologies, and thus misses opportunities for new enterprise value creation. The eight-volume study report identified the principles and practices of Digital Trust, and showed that Digital Trust is already delivering payoffs to companies and government organizations around the world. And, while a true Digital Trust strategy targets value creation, first, information risk reduction and compliance reinforcement always seem to follow as a natural consequence.





It is the *intersection* of these two digital realities — one (the never-ending stream of compliance requirements), so familiar to the insurance industry, and another (value creation through security service and technology), so new to all digital enterprises — that offers a fresh way to plan and direct the investments needed to “secure” the digital enterprise for insurance carriers. Combining the insurance industry’s compliance and security obligations with a mandate for value creation is the motivation for Digital Trust for Life, a research project conducted jointly by CSC and the American Council of Life Insurers (ACLI).

According to the original Digital Trust study, a digital trust security technology strategy aims first at value creation for the enterprise, *knowing* that enterprise information risk will be reduced as a natural consequence. Digital Trust for Life examines that reality in the context of value created for insurance companies, distributors and consumers, with risk exposure reduced and compliance improved as (but) one outcome. The ultimate conclusion is this: *Done correctly, investments normally devoted exclusively to IT compliance and security can, in fact, drive new business value for the insurance industry and deliver the compliance improvements as a natural and valuable corollary.*

The reality of digital trust is indeed, available to the insurance industry.

Questions Asked ...

How can carriers who have historically invested large sums in compliance better target that investment without jeopardizing compliance outcomes? And, how can security in the digital enterprise contribute to growth and competitive advantage, instead of just adding constraints to designs, implementations or operations? Finally, how is it possible for security to improve the efficiency, effectiveness and attractiveness of the carrier enterprise on behalf of an increasingly mobile and geographically independent distribution force?

The Digital Trust for Life project was conducted to answer these and other questions. The specific objectives of the project were framed by a voting process conducted among attendees at the January 2008 ACLI Executive Round Table (ERT), following a digital trust briefing session. Three specific growth and service improvement value objectives were chosen at the ERT. Those original objectives ultimately coalesced into two value objectives centering on customer service and distribution management, and on organic growth and competitive advantage — objectives that sound foreign in the traditional context of security and compliance but ones that are precisely the stuff of digital trust. Those objectives provided the value creation targets for the Digital Trust for Life project.

For the project, we used published reports, guided interviews with insurance industry IT and business representatives, and our own CSC experience as an IT service provider to the financial industry and as a licensed third party administrator (TPA) for life insurance carriers. We then performed a *digital trust analysis* on a sample of systems already deployed and a *digital trust projection* over those same systems to see whether payoffs could still be captured with new applications of digital trust strategies, practices and principles.

... and Answered

Our sample was composed of actual case studies from multiple insurance carriers. While numerically small, the sample was representative of the state of the practice in automated support for customers and agents. The projects in our sample that had been deployed (or were contemplated) were impressive in their own right. Portals, event reminders, status checkers and mobile access for producers were typical, as were faster development platforms, simple online working aids for product examination and comparison, and more comprehensive and engaging automated (online) forms completion and process flow monitoring and acceleration. And, these systems were deployed in full



compliance with regulatory and statutory mandates as well as all company policies and standards. So, industry IT security has done its assigned job well — i.e., keeping IT compliant.

However, security had not been the “lead” in any of the projects, and compliance was normally pursued as an adjunct “checklist” arrangement. Occasionally, security staff suggested a technique or product or technical approach that would make the resulting system acceptable to the compliance checklist. Consequently, any value created for the enterprise came not from security, but from other IT and functional specialties.

In the original Digital Trust study, digital trust was shown to be at work all around the world in just about every industry segment examined. New value was being created in the form of real payoffs that made a difference to the business. For example, the following were all delivered with applications of digital trust: payoffs in increased revenue generation, productivity (doing more for less), efficiency (doing more in less time), new market access and improved sales conversion rates, repackaging and reuse of existing intellectual property to make and sell new products and services, and competitive advantage (market share). The size of the measured payoffs varied greatly, ranging from 20-70 percent in the best examples and as high as 99 percent in one case. Many other payoffs to the business were evident but were not measured by the enterprise. Furthermore, all of these payoffs were accompanied by a reduction in information risk exposure for the enterprise.

Is there something unique about the life and annuity industry that prevents digital trust from delivering payoffs here as well? In the Digital Trust for Life study, the answer is best summed up as:

“No ... just not yet.”

Digital Trust Potential

Notwithstanding the absence of direct evidence of a digital trust strategy at work in any of the companies or case studies examined, there are some very encouraging discoveries. Under the examination of a digital trust projection, the systems already deployed *also displayed the seeds of additional value payoffs* from a fresh application of digital trust principles and practices. There are “value possibilities” that can be sought and captured even from systems that are already deployed. Moreover, in some cases, those value possibilities would seem to be substantial, depending on the specific value objectives and operating circumstances of the individual company making use of the system.

Pursuing Enterprise Value with Digital Trust

Capturing value potential with digital trust is not automatic. Adopting a digital trust strategy for the enterprise requires changes in security organization, security team composition, IT risk governance, security project definition, and the ways in which security requirements, features, functions and technologies are identified, examined or chosen. However, there are two concrete steps that the life and annuity industry can take right now to seek payoffs from typical systems already deployed or in the design process.

1. *Alter the IT risk governance model to include enterprise value creation as an objective.* For life and annuity companies, this means changing the traditional role of security as “gatekeeper” to one of “value creator” — from attempting to police the IT investment to sustain regulatory compliance, to delivering new enterprise value while at the same time reducing enterprise risk and improving compliance as an outcome. This step moves IT security teams to change the way projects are approached and priorities are established. This also forces security teams to address the business needs of the enterprise and start



using a business “translation” of objectives as the basis for security analysis and design, rather than simply repeating the same functional or operational objectives for security, independent of the underlying business objectives. All of a sudden, IT security teams are now asked to create value ... just like everybody else in the enterprise!

2. *Apply a digital trust projection to deployed systems.* Concentrate first on those value creation avenues that have already proven so successful in other industries and which seem directly relevant to the systems and value objectives targeted in this study.⁴ Seven specific avenues of value creation are identified in this study by projecting known digital trust technology capabilities onto the dual objectives of (a) customer service and distribution management and (b) organic growth and competitive advantage. These existing system investments can be extended to create value with digital trust.

Now, More Than Ever

Even before the recent global financial turmoil, digital trust strategy for value creation with security services and technologies made sense. Why would we exempt our security teams from creating enterprise value when we expect everybody else to contribute?

But today, the twin needs to add financial strength to the balance sheet and to improve trust (including digital trust) in business transactions have been amplified many times over. It no longer is enough for IT security to perform only its historical duty of compliance enforcement.

Now more than ever, all parts of the enterprise, including IT security, must contribute real value to the enterprise without elevating information risk or jeopardizing compliance. Digital trust is the way to start doing just that. The demonstrated payoffs in other industries are compelling, and the evidence to date indicates that the life and annuity industry can capitalize as well. Done correctly, establishing a digital trust strategy can become a source of competitive advantage and can help insurers to grow their business while still paying attention to the inevitable tide of new regulations.



PUTTING “LIFE” INTO DIGITAL TRUST

The Beginning

What would your industry do if it discovered a way to “enhance business value with security technology and services — while at the same time tending to important information risks”?⁵ If your industry is one that lives at the intersection of “trust and payoff,” then this discovery would be nearly irresistible ... *but only if* the reality worked for the circumstances of your industry.

This is precisely the condition that stimulated the beginning of the Digital Trust for Life project as a joint activity between CSC and the ACLI. CSC had delivered a brief summary of its digital trust research program during the ACLI Executive Roundtable (ERT) in January 2008. (A summary of results of the original Digital Trust study is provided in Appendix A. All of the research volumes are available without registration or charge at csc.com.⁶) Explanations and examples of digital trust technology at work were included in that presentation. Those examples covered many different industries in many different locations around the globe. But, questions remained about how the reality of digital trust would look against the interests of the life and annuity industry.

This desire on the part of executive roundtable attendees to see how digital trust could manifest itself in life and annuity enterprises led to the start of the Digital Trust for Life project, with dual goals:

- *To examine the application of digital trust specifically for the life and annuity industry*
- *To identify the digital trust technologies that might deliver the most payoff value to in view of the life and annuity industry’s circumstances*

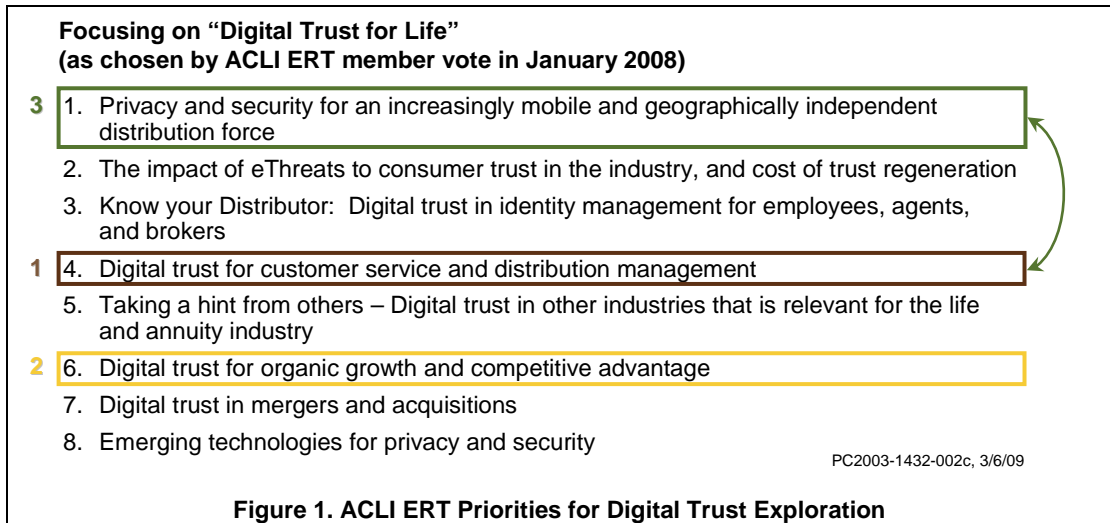
However, Digital Trust for Life project initiation went beyond the articulation of general goals: The executive roundtable attendees had more specific directions to give to the combined project team.

Life and Annuity “Value Objectives”

At the conclusion of the summary briefing, the attendees at the executive roundtable were presented with a list of industry issues that were suggested as target objectives for a digital trust exploration. The list had been generated by CSC industry analysts and executives who planned and operated CSC’s life policy administrator service (a business process outsourcing, or BPO, offering), which was already administering over three million policies from more than 20 carriers. This created a draft list of potential objectives that: (1) represented real business interests of life and annuity industry companies; and, (2) did not need the typical “achieve compliance...” objective that so often distracts value-oriented study projects.

Executive roundtable attendees voted their preferences from the full list of eight choices as shown in Figure 1. After three rounds of voting, attendees prioritized their top three choices. These top three issues became the “value objectives” that shaped and targeted the digital trust analysis in the Digital Trust for Life project.

All three issues are closely related and reflect a consistent theme of growth and productivity. During the study, however, the linkage between value objectives 1 and 3 grew stronger and stronger, eventually blurring any real distinction between the two. So, during the bulk of the study, the real focus was placed on value objectives 1 and 2 — i.e., digital trust for customer service and distribution management, and digital trust for organic growth and competitive advantage.



None of the eight objectives shown in Figure 1 describes an exclusive effort to “achieve compliance.” That observation reflects one of the four strategic conclusions of the original Digital Trust study ⁷, namely:

“Aim high and first with a digital trust strategy to get the payoffs.”

This conclusion includes the digital trust reality that risk exposure is reduced as a natural consequence of “aiming first for payoffs,” ultimately leading to improved compliance. So, with digital trust there need not be a “compliance objective” in the list. Such an omission is clearly foreign to traditional security analysis studies, but it is precisely the nature and advantage of digital trust. In fact, it is this reality that guarantees that the important industry intersection of “compliance requirements” and “value creation needs” will be addressed ... *regardless of which value objectives had been chosen by the executive roundtable attendees!*

Payoffs

Traditional Information Risk Management

Even traditional security analysis and management techniques frequently claim a “value proposition” in return for following a recommended action. That value proposition is often expressed with one or more statements regarding:

- Improved compliance (“we must do this”)
- Additional certifications or accreditations (e.g., certified PCI DSS compliant)
- Improved security posture (e.g., greater and faster access to security status information in dashboards or reports)
- Implementation of a “best practice” (e.g., aligning the security program with ISO 27001 and 27002)
- Reduced cost for some necessary capability already being performed (e.g., automated vulnerability scanning)
- Extensions of a current capability already being performed (e.g., user authentication extended from laptops to smartphones)



These are all familiar propositions, suggesting very “good” outcomes. But, other than potential cost reductions, none of them create new value for the enterprise. Rather, in keeping with the traditional formulas of classical information risk management,⁸ they all claim only incremental improvements in risk reduction for the enterprise value that already exists. Consequently, they are all reflections of an approach that makes security just “the cost of doing business” — a necessary expenditure for an effort somehow exempt from the enterprise call to create value for clients, employees and stakeholders of all kinds.

Digital Trust Dividends

On the other hand, digital trust is about more than dealing with the risk of loss. Digital trust impacts the *business* of the enterprise, not just the network topology or the security software inventory or the policy enforcement process or even the enterprise risk profile. So, the payoff targets for digital trust — i.e., the dividends — are value creation that makes a real difference to the business. It is a further reality of digital trust that such value creation also leads to risk reduction.

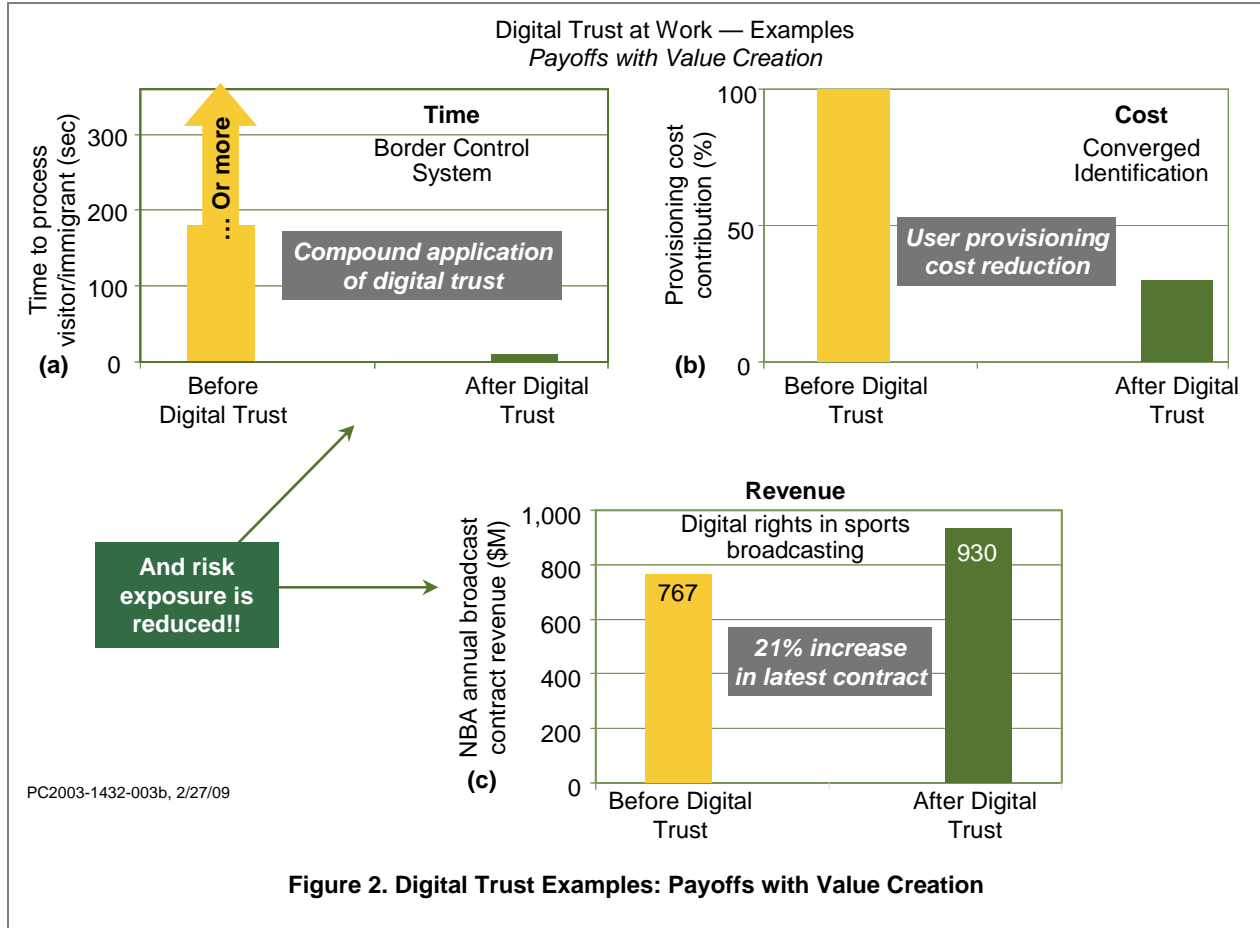
In the original Digital Trust study, digital trust dividends included such payoffs as increased revenue generation, productivity (doing more for less), efficiency (doing more in less time), new market access, improved sales conversion rates, repackaging and reuse of existing intellectual property to make and sell new products and services, and competitive advantage (market share). The size of measured payoffs varied greatly, ranging from 20–70 percent in the best examples, with a few over 90 percent! Many other payoffs to the business were evident but not measured by the enterprise. Furthermore, payoffs were apparent in every region of the globe and in every industry examined.

Figure 2 shows a sample of three different kinds of payoffs generated by digital trust and reported in the original study. While the payoffs themselves are substantial, it is important to note that *risk exposure is also reduced* as a beneficial consequence of “aiming at value creation.” This again illustrates a remarkable reality of digital trust:

A digital trust strategy for enterprise value creation almost always brings information risk management “reduction in risk of loss” as a natural consequence.⁹



And, a reduction in risk exposure leads to improved compliance. In other words, when done correctly, digital trust not only moves us to greater compliance, but does so as a beneficial consequence of first concentrating on enterprise value creation.



This reality was seen over and over in every industry examined. And, compound applications of digital trust technologies as illustrated in example (a) of Figure 2 delivered the greatest measured value creation. While such compound applications of digital trust were not explicitly studied in the original effort, there is anecdotal evidence that they also delivered the greatest improvement in risk exposure. Based on these earlier results, the working hypothesis in the Digital Trust for Life study is that the life and annuity industry is not immune from the realities of digital trust, and therefore it should be able to apply the principles and practices of digital trust to achieve the same kinds of dividends as seen in other industries.

Digital Trust Deficits

So, “having” digital trust is clearly a good thing, with dividends of real value to the enterprise, along with reductions in risk exposure and consequential improvements in compliance. But the original study also showed that real penalties accompany digital trust deficits.

The clearest examples of penalties accompanying digital trust deficits are those associated with a lack of compliance. There are certainly other types of painful penalties including exclusion from the market,¹⁰ reduced sales conversion rates,¹¹ and the loss of intellectual property and licensing



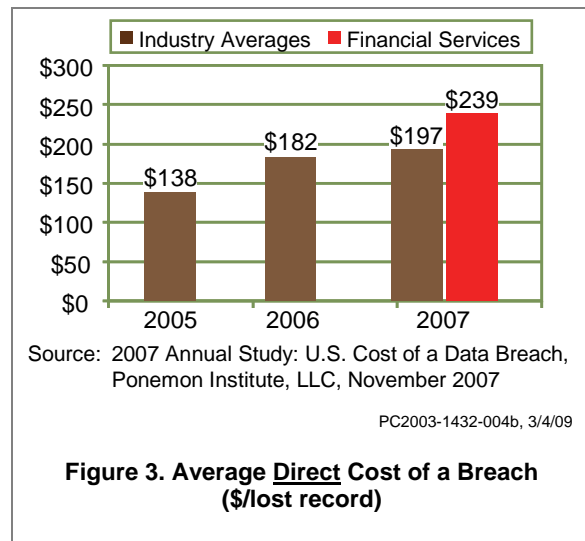
revenue.¹² In fact, the life and annuity industry suffers a particular online penalty due to digital trust deficits. In its Third Quarter 2008 Online Customer Respect Study of Life Insurance Industry Websites, The Customer Respect Group noted “not enough attention to trust” (i.e., digital trust) for industry websites, and concluded that such a digital trust “deficit” was delivering a penalty to the industry in the form of a shortage of good leads for offline business.¹³

However, the number and variety of compliance mandates makes digital trust deficits in this category especially dangerous. The introduction of privacy breach laws in (currently) 44 states, the District of Columbia, Puerto Rico, and the Virgin Islands¹⁴ has complicated compliance still further in the United States, and has led to many high-profile failures across industry sectors. For instance, nearly every history of compliance includes the story of TJX and its privacy compliance failure.¹⁵ That single episode of a digital trust technology deficit (in wireless security) cost TJX over \$125 million in direct penalties, plus unmeasured (but painful, nonetheless) indirect penalties of lost business and a depressed stock price.¹⁶

Compliance Penalty Potential in the Life and Annuity Industry

Certainly the life and annuity industry is no stranger to compliance, with both state and federal regulators involved in a host of laws, rules, and standards. With so many regulatory and licensing mandates, it is hard to overstate the significance of compliance to the industry. Furthermore, regulatory circumstances are bound to change as time goes on. Even before the current financial crisis, such regulatory proposals as the Optional Federal Charter, the Office of Insurance Information and the National Association of Registered Agents and Brokers had all been introduced and/or passed in one or more houses of Congress. Given the expectations for the new presidential administration, all sorts of changes could be swept up in major federal regulatory reform.

Notwithstanding the importance of all the other regulatory proposals, the privacy breach obligation is a good illustration of the sensitivity and importance (and fluidity) of compliance, particularly to the life and annuity industry. As shown in Figure 3, the direct penalties due to privacy breaches are up 43 percent since 2005. Further, in 2007 the news for financial services was 21 percent worse than the overall average! Moreover, according to the Ponemon Institute, about 65 percent of those costs are due to lost business¹⁷ — certainly a penalty that harms any attempt at “organic growth and competitive advantage.”

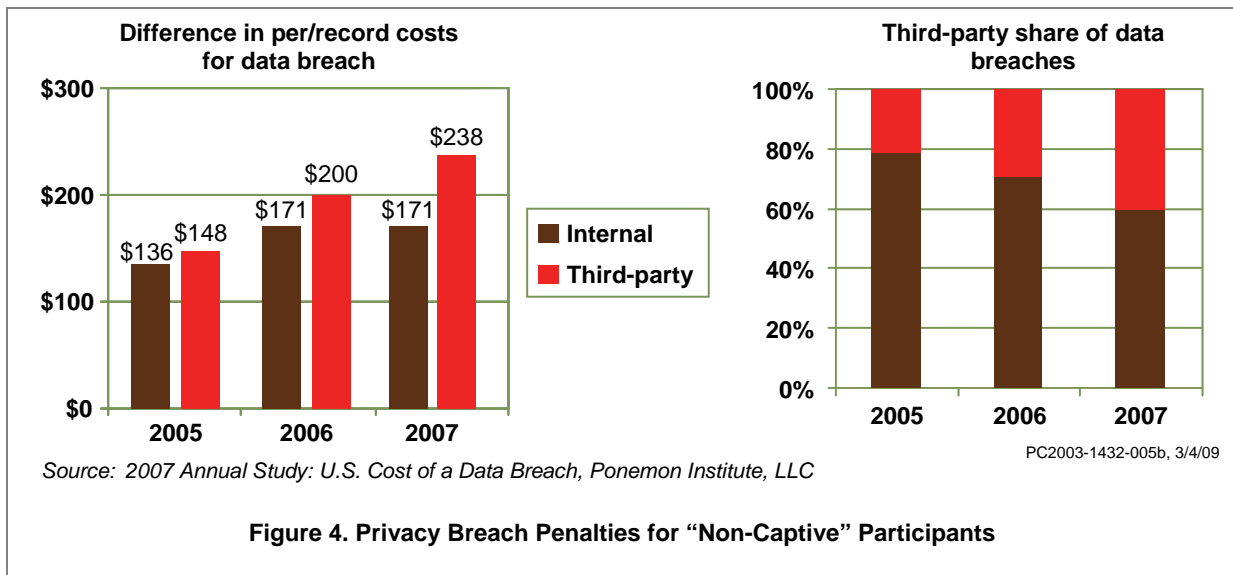


In addition to these *direct* penalties, there are also *indirect* penalties. Though not specific to the financial services industry, they are important nonetheless. For example, a study in 2006 by Enterprise Management Associates of companies whose compliance failure could be traced to information security breaches showed that stock prices fell by an average of 5 percent within a month of disclosure of the failure and remained 2.4–8.5 percent below the pre-disclosure (pre-compliance failure) prices for another 8 months. Furthermore, prices did not recover for nearly a year.¹⁸ And, on



top of all this, earlier studies by A.R.C. Morgan in 2004 on related events showed such unpleasant circumstances as a tripling of the growth of audit fees, a restatement of earnings and the resignation of CFOs.¹⁹

Figure 4 also shows another disturbing circumstance regarding privacy breaches for all industries where third parties (i.e., non-employees) are directly involved in the business chain. The data of Figure 4 indicate that third parties have doubled as the source of data breaches from 2005 to 2007, and that the cost difference has increased by 450 percent in that same timeframe! So, carriers who use non-captive agents would seem to be even more vulnerable to a privacy breach and the increased penalty costs of response.



However we choose to interpret data for privacy breaches or any other compliance mandate for the life and annuity industry, the facts indicate that compliance needs will never end. Indeed, today's trend is that the compliance spend will have to increase!²⁰

This, then, is the situation that amplifies the importance of this Digital Trust for Life study beyond the general goals established earlier.²¹ With no regulatory relief in sight, is this current (never-ending) investment in IT compliance just "the cost of doing business?" Is there no better way for carriers, who continue to invest large sums in compliance and security for the digital enterprise, to reap enterprise value from that investment?

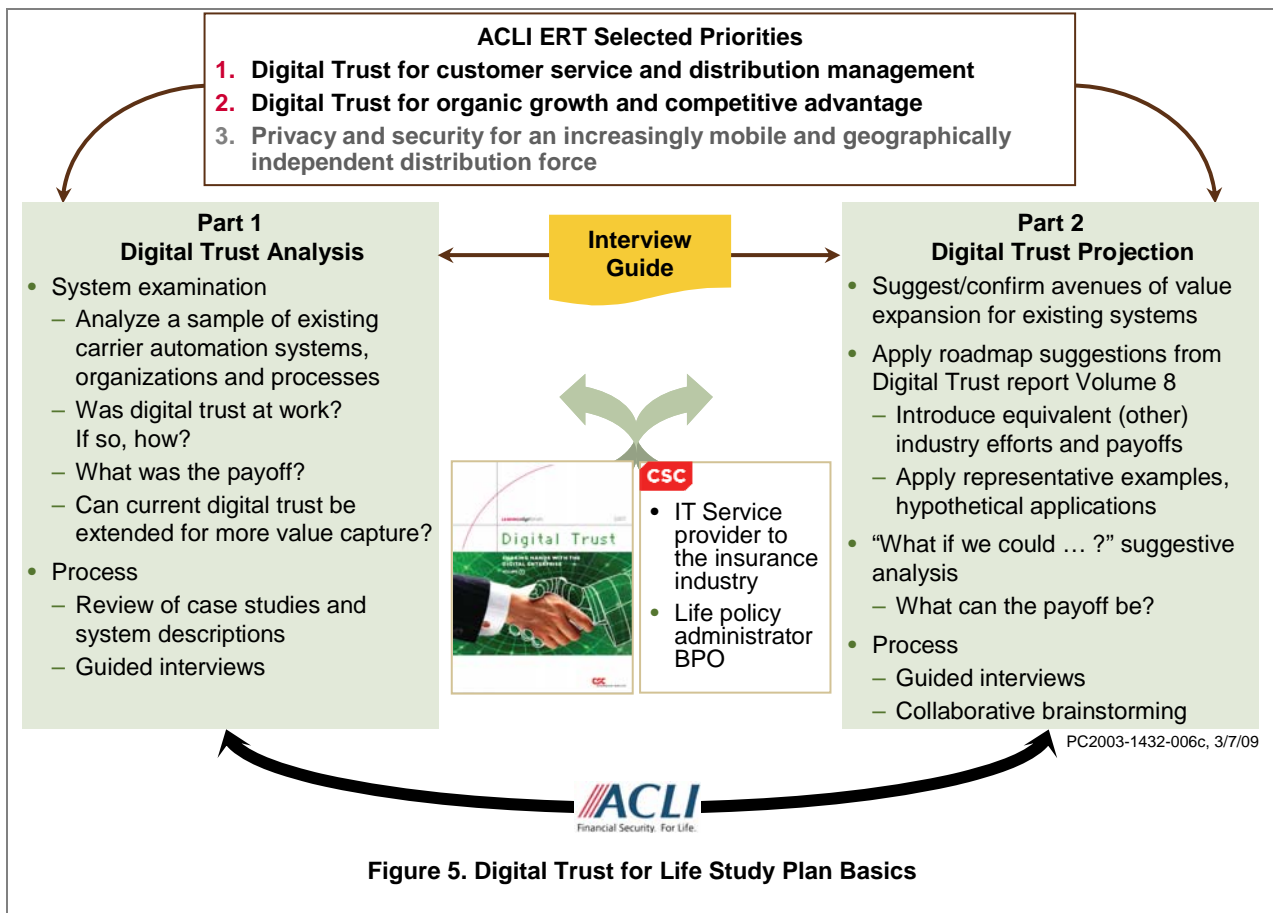
What can digital trust do for the life and annuity industry?



DOING “DIGITAL TRUST FOR LIFE”

The Study Plan

The Digital Trust for Life project was conducted in two main parts following the selection of the value objectives at the ACLI ERT. As illustrated in Figure 5, both parts were reinforced by the results of the initial Digital Trust study and by the industry knowledge and work history of CSC’s own IT service teams and its BPO for life policy administration. Furthermore, ACLI encouragement to member companies to support the study effort smoothed the path to interviews with IT and security leaders, and helped to get accurate and candid information about actual implementations and case histories. All information used in the study was either already public information or was volunteered by the study participants during conversations and subsequent information exchange sessions.



Industry Interviews and Conversations

In order to simplify the descriptions of purpose and objective for industry study participants, and in light of the convergence of three original value objectives into two, we prepared a single mission statement to capture the intent of all value objectives, and then followed a field study process as shown in Figure 6. The mission statement for the Digital Trust for Life project became:

“Apply security technology and services that stimulate organic growth and competitive advantage through a reliable, mobile and (even) independent yet enthusiastic distribution



and customer service force, while reducing the chances of improper information usage or disclosure.”

That statement, along with a brief abstract of the original Digital Trust study, introduced our request for support from industry participants. Mindful of the time constraints any industry participant would have, we combined those two working aids with a Digital Trust Interview Guide that helped to shape conversations, keep the discussions on point and capture the kinds of information we needed to perform both Part 1 (Digital Trust Analysis) and Part 2 (Digital Trust Projection) based on the information from a single conversation with each participant. As illustrated in Figure 6, sometimes there were follow-up e-mail exchanges, and occasionally, information discoveries would require some conclusions and actions to be rethought or refined to incorporate the new data. By and large, however, advance preparation prior to any conversations or interviews, combined with the items in the study toolkit, made it possible to gather most of the desired information in single 1-2 hour conversations with volunteer participants from carrier IT and security organizations.

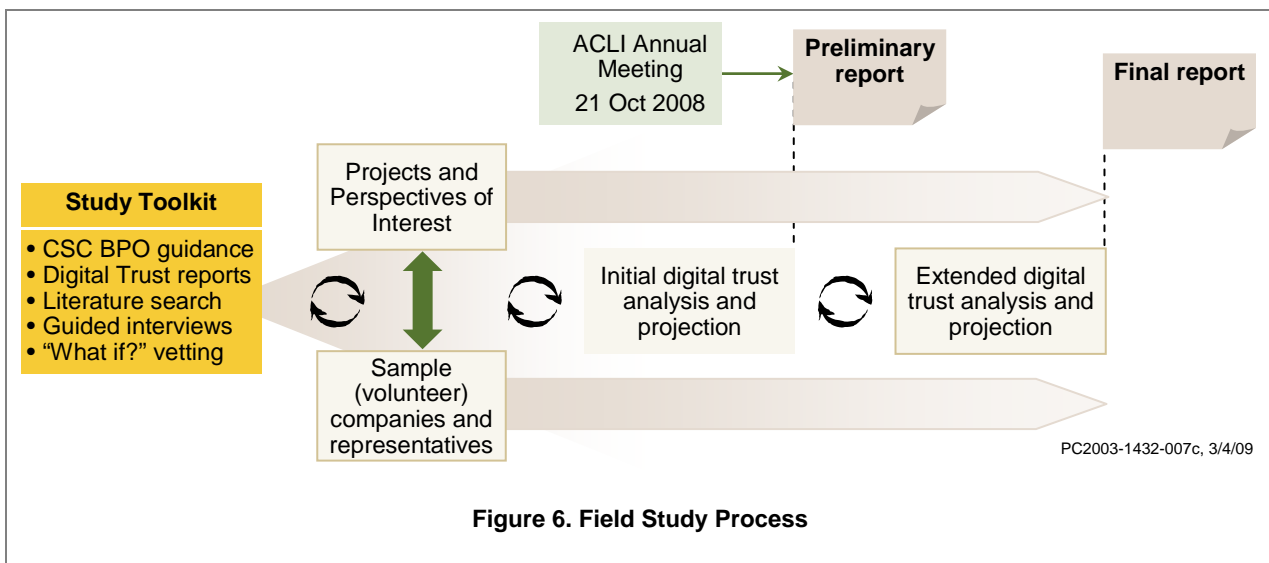


Figure 6. Field Study Process

Industry volunteers for interview and information exchange as part of the Digital Trust for Life project were initially sought by canvassing those company contacts already known to CSC through its IT and BPO service functions. Later, this canvas group was expanded by references from others who had been contacted. No carrier willing to participate was excluded. As expected, the most useful contributions came from carriers who had one or both of the following characteristics:

- Known deployments of automated systems that had exhibited payoff potential for their enterprise
- A history and expression of interest in pushing information security organizations and functions to have a role other than their traditional compliance mandate

Reporting

Most of the data collection and analysis was conducted during summer 2008. Two reports were planned: The Preliminary Report on the project was given in a briefing on October 21, 2008 during the ACL I Annual Meeting in Boston. This document is the Final Report.



Part 1 — Digital Trust Analysis

Digital trust analysis across both value objectives was performed in tandem. The close linkage of the value objectives (see “Life and Annuity Value Objectives” on p.8) made such a concurrent analysis an easy and natural process.

However, as listed in Figure 7, the plans and systems used as objects of the analysis were divided into two broad categories, field force and customers, each of which roughly matched one of the value objectives.

Furthermore, since this particular analysis of digital trust was directed at

an *industry* conclusion, rather than an *individual enterprise* conclusion, the systems examined have been presented in this report as representative characterizations of multiple case studies, converged around typical feature, function and capability sets.

Value Objective	System Category
Customer Service and Distribution Management	Electronic platforms for the field force
Organic Growth and Competitive Advantage	Electronic platforms for customers

Figure 7. System Categories for Digital Trust Analysis

Notwithstanding this categorization, it is evident that services in each system category can contribute to both value objectives in one way or another. For example, it is hard to imagine how an automated system that helps producers be faster and more accurate in contract preparation would not also help “organic growth and competitive advantage.” Likewise, it is equally hard to imagine how a system that helps customers make decisions more quickly about annuities and retirement plans (and take immediate action on those decisions) would not also contribute to the improvement of “customer service and distribution management.”

Despite these clear linkages, the category distinctions are useful in the examination and analysis process. They are also useful to help spot missed opportunities and the Part 2 effort for digital trust projection. However, such distinctions did not materially affect the conclusions of the digital trust analysis (or projection) across the board. That is, *both categories of systems examined in light of each value objective delivered essentially the same digital trust conclusions.*

Customer Service and Distribution Management

A handful of fully operational automated systems that provide support or improvement for “customer service and distribution management” were examined for evidence of digital trust strategy or practice already being used. While there were differences in the specifics of each system examined, they were all aimed at making agents more:

- More Effective (sell/service better)
- More Efficient (sell/service more quickly)
- More Attractive (sell/service for me rather than for other carriers)



Certainly they were intended to provide some differentiation in the marketplace as well. All of the cases could be described within the general terms of “agent portal” (either an information portal or a transactional producer portal) or some form of an “electronic agent platform.” While the number of actual cases examined in the Digital Trust for Life project was small, these findings are representative of the state of the practice in the insurance industry according to such industry monitors as Celent.²² In fact, as highlighted in Figure 8, recent studies of the deployment of technologies supporting customer service and distribution management show that portals have become the standard technology for producer support. In addition, CSC reports that over 50 percent of the carriers visited by CSC have, or are developing, an electronic agent platform for new business.²³

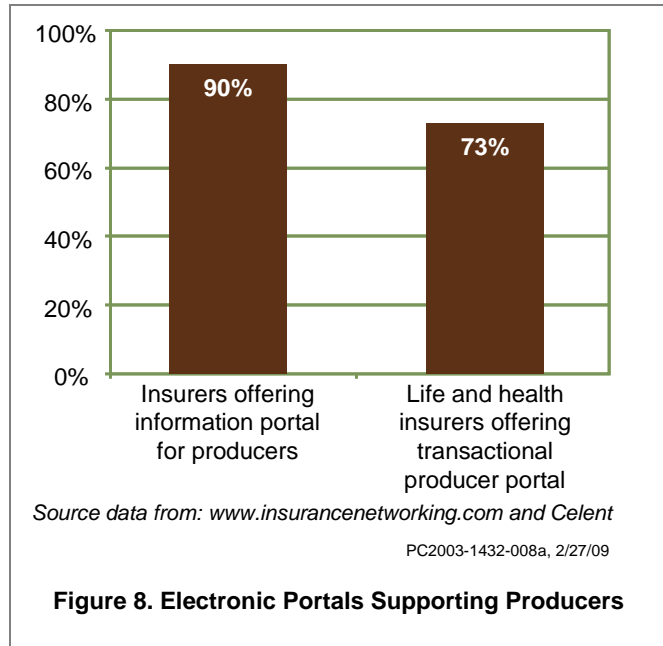


Figure 8. Electronic Portals Supporting Producers

Portal Systems Supporting Producers

Figure 9 characterizes the collection of portal systems examined. These systems are wonderful examples of Web technologies and mobility technologies applied by the carriers to support and accelerate the operational needs of the field force.



(1) Application*	(2) Objective	(3) Traditional Security Analysis	(4) Typical Business Payoffs (anecdotal)	(5) Compliance Payoffs (inferred)
	<ul style="list-style-type: none"> Subscription-based Web portal for agents Notifications of policy or business events 	<ul style="list-style-type: none"> Identification and authentication for mobile operations and devices Confidentiality for information in transit and at rest (on mobile device) Transaction auditing 	<ul style="list-style-type: none"> Agents are more efficient and effective Business is "easier to do" 	<ul style="list-style-type: none"> "Better"
	<ul style="list-style-type: none"> Mobility applications to bring client data to the handheld 	<ul style="list-style-type: none"> Identification and authentication for mobile operations and devices Confidentiality for information in transit and at rest (on mobile device) Transaction auditing 	<ul style="list-style-type: none"> Available to entire company field force "Saved an account" with mobile access 	<ul style="list-style-type: none"> "Better"

*Converged characterizations of actual case studies from multiple insurance carriers

PC2003-1432-009c, 3/4/09

Figure 9. Digital Trust Analysis of a Converged Representation of "Portal Systems" Supporting Producers (the Field Force)

There were multiple types of "portals" targeting different objectives, as shown in Figure 9. Some were aimed more at keeping agents informed of important policy and business events related to their customers, while others were aimed at loosening the bonds of device dependence. In the latter case, agents are able to query client data repositories from a variety of portable and ultra-portable devices, and give "on the spot" answers to clients.

Electronic Agent Platforms

Figure 10 shows an equivalent result for the development and deployment of electronic agent platforms in support of "customer service and distribution management." Once again, these systems are fine examples of automation in support of the agent processes involved in selecting, filling in, filing and reporting the various forms that are needed to complete an insurance application or adjust a retirement plan contribution. In this category, however, some carriers have actually measured the payoffs attributed to these systems. As listed in columns 4 and 5 of Figure 10, the business payoffs have been measured in millions of dollars per year, and compliance payoffs measured by a reduction in the penalty costs from Market Conduct Examinations. In one case, home office cost reductions for the field agent force were on the order of \$5 million per year, and reduction in field office staff time was valued at \$27 million annually for financial representatives.



(1) Application*	(2) Objective	(3) Traditional Security Analysis	(4) Typical Business Payoffs	(5) Compliance Payoffs
<p>Thick client laptop agent</p> <ul style="list-style-type: none"> • Captive agents only • Single, tightly-controlled desktop configuration 	<ul style="list-style-type: none"> • Mobile laptop-based platform for field agent force • Electronic application for insurance at customer's home or workplace 	<ul style="list-style-type: none"> • Identification and authentication for captive agents • Confidentiality for information in transit and at rest (on mobile device) • Configuration compliance • Transaction auditing 	<ul style="list-style-type: none"> • Reduction of home office staff costs (measured in \$M) • Reduction of field office staff time (estimated at 1-3 hours/day of forms and prep work) • Improved underwriter and processor productivity 	<ul style="list-style-type: none"> • Reduced penalties from Market Conduct Examinations (measured)

* Converged characterizations of actual case studies from multiple insurance carriers

PC2003-1432-010d, 3/6/09

Figure 10. Digital Trust Analysis of a Converged Representation of “Electronic agent Platforms” Supporting Producers (the Field Force)

Organic Growth and Competitive Advantage

In like manner, a sample of industry systems planned or deployed for “customer support” were also examined for evidence of digital trust strategy or practice already in use. Systems were chosen both for conformance to the value objective and for availability of information about what they do, how they work and what benefits (especially measured benefits) have accrued. In particular, systems supported the business priorities of:

- Generating new, better products faster than the competition
- Improving the ratio of sales conversions
- Improving the average size of products sold
- Making the buy/sell decision and transaction faster and easier to complete (for the customer)

As usual, all of these characteristics are tempered by the recognition that sales and service are traditionally done through a Personal Producing General Agent (PPGA), but that fully online self-service models are now in place with some carriers, particularly for smaller, simpler products (e.g., term life insurance).²⁴ Even without fully online product availability, the quest for “straight through processing” (STP) and faster closure has already led to the use of electronic signatures (with and without special hardware) and interactive, online customer support.

Moreover, with individual state approval required for each new product developed, the System for Electronic Rate and Form Filing (SERFF) has continued to gain popularity. Today, all 50 states, the District of Columbia, Puerto Rico and over 3,000 insurance companies, third-party filers, rating organizations and others are already committed to SERFF.²⁵ These kinds of actions are clear industry attempts to improve “organic growth and competitive advantage,” but they are not necessarily examples of digital trust. Figures 11 and 12 illustrate two of the most popular electronic system types deployed in support of “organic growth and competitive advantage.”



Decision Support and Transaction Initiation

Figure 11 highlights interactive techniques to engage clients (and potential clients) in instructional and “what if” scenarios to help them make decisions about insurance and retirement plan contributions. If decisions result in a change of election, then that change can be captured electronically, and ultimately (usually at a later time) forwarded to a central processing site for final processing and execution. One example of this particular variety of customer support platform has delivered business payoffs that include enrollment rates exceeding 90 percent and savings rates being increased by an average of over 5 percent beyond earlier elections.²⁶ In all cases examined, the compliance payoffs could only be inferred to be “better”.

(1) Application*	(2) Objective	(3) Traditional Security Analysis	(4) Typical Business Payoffs	(5) Compliance Payoffs (inferred)
<p>Enrollment status and alternative exploration and purchase</p> <p>Client Enrollment Information</p> <ul style="list-style-type: none"> • Enrollment status • Alternatives • Options, risks • Goal setting 	<ul style="list-style-type: none"> • Engage customers with hands-on manipulation of alternatives and retirement planning • Encourage instant commitment to purchase without delay for forms or other paperwork 	<ul style="list-style-type: none"> • Identification and authentication of clients and session lead • Confidentiality for information in wireless transit and at rest (on mobile devices) • Configuration compliance • Transaction auditing and reporting 	<ul style="list-style-type: none"> • Average on-site enrollment rate increased • Initial contribution rate is larger • Large majority of participants who are already contributing increase their savings rate still further (to an average of 8%) 	<ul style="list-style-type: none"> • “Better”

* Converged characterizations of actual case studies from multiple insurance carriers


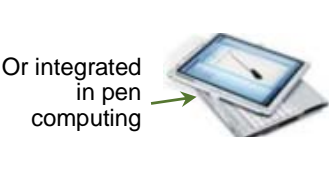
PC2003-1432-011c, 3/6/09

Figure 11. Electronic Decision Support and Transaction Initiation Platforms for Customers

Electronic Product Selection and Transaction Completion

Figure 12 illustrates the systems that bring all the pieces together for client decisions and complete execution of those decisions. As suggested in column 2 of Figure 12, various versions of this system type can support some or all of the sales and contract execution steps, from needs analysis and comparison to contract signing and payment collection.²⁷ Many systems of this type include a member of the field force to help complete the transaction (e.g., obtaining the signature), while others can operate in a “self-service” mode for some of the simpler products.²⁴ Even for some of the earlier systems deployed, the business payoffs (column 4 of Figure 12) are attractive. Anytime the enterprise can speed the sales transaction, increase policy processing productivity, shorten the underwriting timeline, and reduce back office underwriting and underwriting support staff by as much as 30 percent,²⁸ then real business value is certainly being created. Once again, however, compliance payoffs can only be inferred as “better.”



(1) Application*	(2) Objective	(3) Traditional Security Analysis	(4) Typical Business Payoffs	(5) Compliance Payoffs (inferred)
 <p>With or without tablet</p>  <p>Or integrated in pen computing</p>	<ul style="list-style-type: none"> Needs analysis, product selection, generate illustration, complete all applications and forms, pay for coverage, generate contract – all in one transaction 	<ul style="list-style-type: none"> Identification and authentication of clients and agent lead Confidentiality for information as collected, stored, and (ultimately) as transmitted to central office Validity of electronic signatures Configuration compliance Transaction auditing and reporting 	<ul style="list-style-type: none"> Sales experience speeded both in person and on the phone Increase of processing on new life policies by 40% Shave 7 days off the underwriting acceptance process Back office staff reduction 	<ul style="list-style-type: none"> “Better”

* Converged characterizations of actual case studies from multiple insurance carriers

PC2003-1432-012d, 3/6/09

Figure 12. Electronic Product Selection and Transaction Completion Platforms for Customers

Digital Trust in Evidence?

The digital trust analysis effort examined exactly the type of automated systems as would be expected in the industry today in support of the two value objectives. And, despite the general lack of before-and-after business impact and compliance measurements, the payoff indicators shown in columns 4 and 5 of Figures 9 through 12 lead to an enterprise consensus that satisfactory business payoffs have been achieved and compliance is at least “okay” if not “better.” This enterprise consensus is based primarily on anecdotal evidence, buttressed by a few specific empirical measurements and compliance results.

But, was Digital Trust being applied and was value being generated as a result? Was Digital Trust already at work within the industry? Was the value outcome *all it could have been* based on the lessons of a Digital Trust strategy and practice?

Still the “Gatekeeper” Model

Whatever payoffs are acknowledged as being achieved through these system deployments, *it does not appear that digital trust strategies, principles or practices were at work in any of them.* The analysis indicates that the security teams that worked on these systems applied a thorough, time-tested security evaluation aimed exclusively at compliance obligations. In this traditional style of security service, the role of security is one of “gatekeeper.” As highlighted in column 3 of Figures 9 through 12, those compliance obligations typically involved configuration correctness, identification and authentication (logging in and providing a password or other authentication factor), making sure that data is encrypted at least in transit and preferably in storage as well, and keeping a record of the events that transpired to verify their correctness or respond to any unexpected or unauthorized actions.

These traditional “gates of compliance” were applied in accordance with enterprise policies by experienced security teams. However, while that gatekeeper role was administered carefully and comprehensively in the systems studied, there were no recorded cases of security teams bringing



additional enterprise value to the system. Typically, the systems were designed and developed by enterprise IT teams to satisfy a (value-producing) need, additional resources were expended to satisfy the compliance rules, and then the system was deployed to reap the originally intended payoffs.

The security teams were involved at different times in the development process (depending on the development model and historical practice of the enterprise), but most of the security effort was applied during the latter stages of development. Sometimes technology and deployment changes were necessary as a result of unsatisfactory compliance findings and judgments. In every case examined, the development team reworked the system to include new capabilities and conditions for compliance. Then the security team re-examined the resulting new version to verify compliance. Security success was defined to be approval for deployment from the enterprise security authorities (e.g., Director of Security, Chief Information Security Officer).

It is clear that these systems do, indeed, generate payoffs for the enterprise. It is also clear that the security teams did exactly as their enterprise practices and risk models directed, using their own careful thought and evaluation techniques. However, analysis also shows that *none of the payoffs identified are attributable to a digital trust strategy*. In fact, a quick scan of column 3 in Figures 9 through 12 reveals a striking uniformity of security actions, *regardless of the application type or objectives*.

Following the conventional wisdom of “best practice,” nearly equivalent kinds of solid traditional security analysis were performed on behalf of a compliance agenda, seemingly independent of the purpose of the system service itself. The gatekeeper model of security service was applied well, since the systems were deployed in full compliance with enterprise policies and mandates. But, in accordance with current carrier roles and assignments for security functions and services, security teams had neither obligation nor opportunity to introduce security technology and features that would add further enterprise value to the system.

Digital Trust Promotes Security Value Identification and Capture

The security teams applied their assigned gatekeeper model of security very successfully — i.e., compliance was achieved. But, no digital trust strategy or practice was applied, so compliance was *all* that was achieved. Earlier studies of digital trust results show that the same compliance target can be met even as additional value is being created with a different application of digital trust technologies and services. Is that result available to systems like these in the life and annuity industry?

In this report, “Part 2 — Digital Trust Projection” deals more completely with digital trust opportunity potential in the life and annuity industry. But, a single example here helps to illustrate the power of digital trust when applied correctly. For instance, Figure 13 contrasts the different results when a digital trust strategy (instead of the gatekeeper model) is applied to enterprise business objectives — like customer service and distribution management. In this example, the “gatekeeper” portion of the illustration is the same composed characterization as was shown in Figure 10. The gatekeeper model successfully targets security and privacy compliance mandates. However, the consequence of the gatekeeper model is that the compliance mandates become system constraints, limiting the population of producers to captive agents, only, and limiting the devices that producers can use to a single type and configuration.

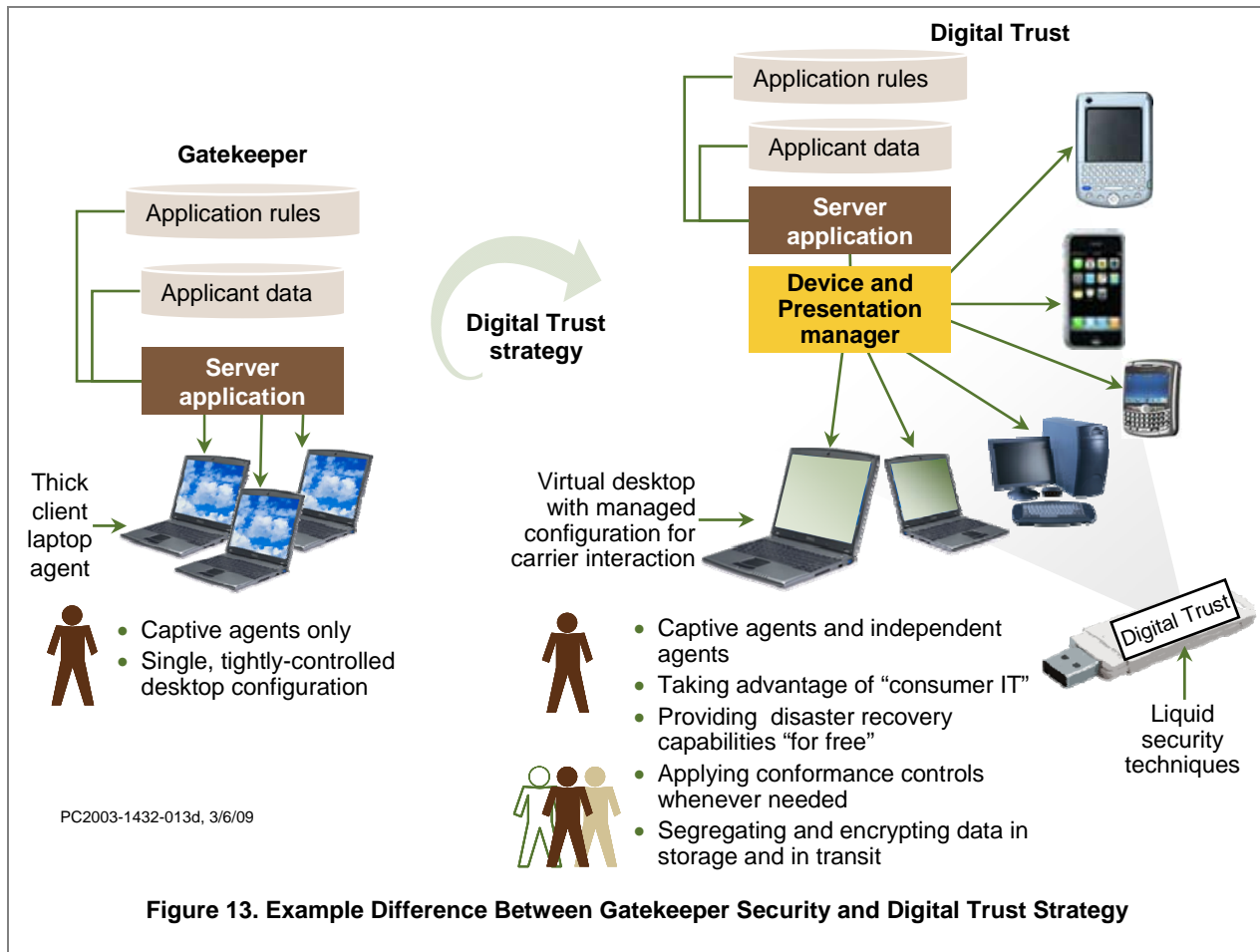


Figure 13. Example Difference Between Gatekeeper Security and Digital Trust Strategy

On the other hand, the digital trust strategy directs security attention to dealing with desired business results, causing the generation of a different security architecture and the selection of different security products. In this case, the outcome is best described in terms of how the *business* is different rather than how *compliance* is achieved. For instance, in the example of Figure 13, “liquid security”²⁹ technologies deliver the business outcomes of:

- Captive agents and independent agents being supported with the same structure

Living on the Web!

One of the first (and still best) examples of the value potential for “liquid security” can be seen in the experience of BP when it started the Digital Allowance Scheme (DAS) for staff in 2005. Under DAS, certain categories of qualified users were allowed to volunteer to be removed from the corporate LAN and operate completely “on the Web.”

Since its initiation, over 18,000 users have been removed from BP corporate LAN infrastructure and support costs, and allowed to use their own equipments and support mechanisms (consumer IT). The DAS contributes a fixed amount of money to each user to be applied as the user sees fit. Furthermore, it is BP’s experience that security (compliance) *improved* with this action!

More about the de-parameterization of the enterprise has been written by members of the Jericho Forum (www.jerichoforum.org).

Adding liquid security to the foundation ideas of the Jericho Forum expands the populations of “qualified users” and increases the value potential many times over.



- “Consumer IT”³⁰ becoming legitimate and useful for personal producing general agents (PPGAs)
- Disaster recovery features (for individual PPGAs) being added “for free”
- Compliance being reinforced

How much value is to be captured in this example? The answer depends on the particular circumstances and business objectives of the carrier that chooses to follow this digital trust strategy. For example, if the carrier were eager to expand the sales force from captive agents to include independent agents as well, and to move beyond the current membership base, then this digital trust strategy would deliver more real business value than for those who sought only to speed information flow and take advantage of consumer IT. However, in almost any circumstance, the value potential in this example is very large. (See “Living on the Web!” sidebar article.³¹) And, while this new value is being captured, risk exposure is being reduced and compliance is being reinforced.

Digital Trust Analysis Results

In like manner, every system examined in the digital trust analysis phase of this study revealed some missed opportunities for security value capture. As wonderful as these systems are, the absence of a digital trust strategy and the omission of important digital trust principles and practices meant that security teams were targeted at compliance ... and only compliance. And, as successful as the security teams were, their designated roles and assignments did not open up important avenues for digital trust. Those revelations not only pointed to consistent threads of constraint, but also to consistent avenues of potential digital trust value capture that overlap both value objectives.

Missed Steps

Different enterprises arrive at digital trust in different ways. A summary set of directions for “doing digital trust” can be found in the *Epilogue and Strategic Roadmap* volume of the original Digital Trust study,³² but that instruction is not prescriptive. Notwithstanding the “many paths” possibilities for evolving to digital trust, the analysis performed on systems in the life and annuity industry did consistently uncover three conditions indicative of “missed steps” for digital trust:

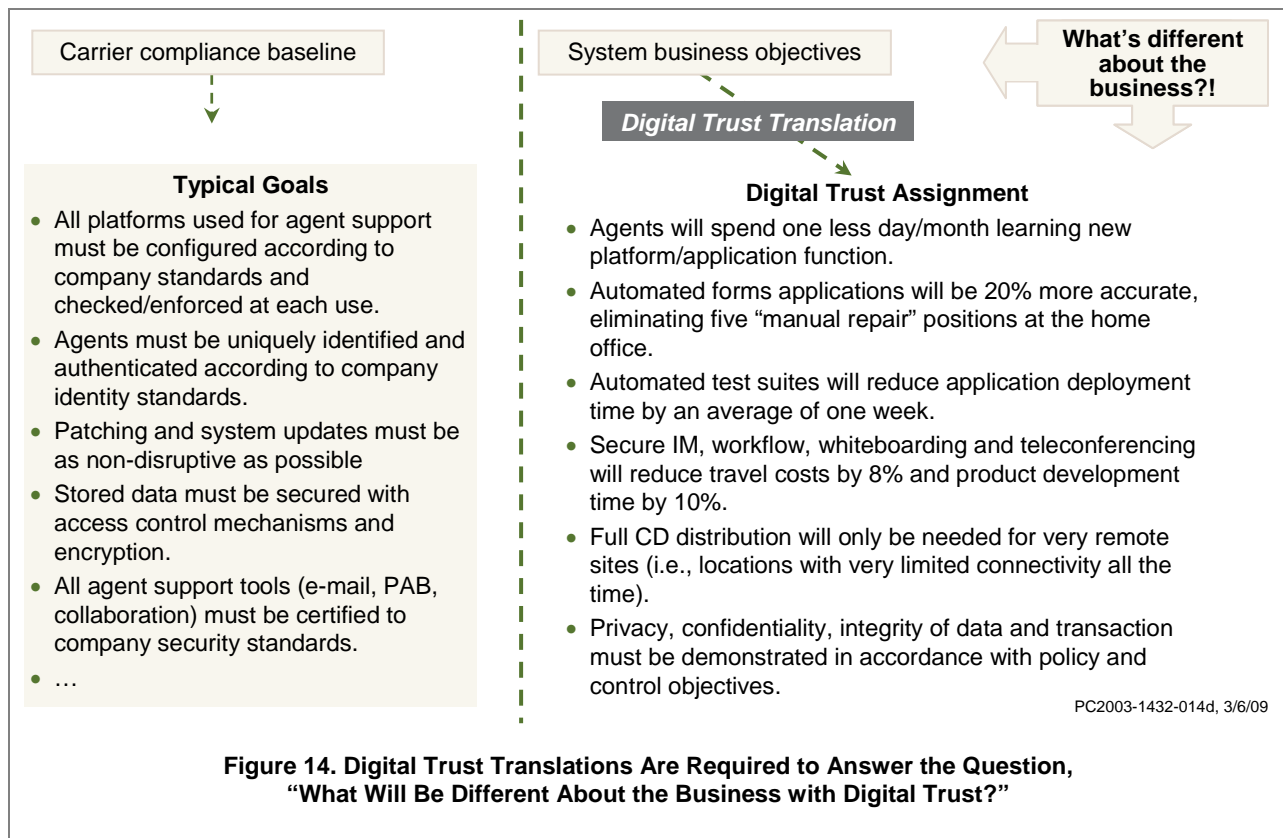
- Security and compliance are worked exclusively as “constraints.”
- Achievement and certification of compliance is the only measurement used to determine if the security teams are doing a good job.
- Security teams have no clear visibility into the business objectives of systems being built and deployed.

Any one of these conditions will block an evolution to digital trust. Although these conditions are not roadblocks to compliance (after all, compliance is being achieved), they prevent the organizational response needed, the performance metrics that stimulate the right actions, and the security technology and process selections from delivering digital trust (i.e., new value and compliance).

One classic observation from the digital trust analysis is that, often, there appeared to be only faint connections from security teams to the real business requirements underpinning system development and deployment. Consequently, security teams responded to the typical operational and compliance requirements with traditional security analysis, techniques, and toolsets. Without that clear connection to business needs, the processes followed and tools chosen and implemented can only be aimed at compliance. Moreover, without that connection, the important value-producing step of translating business requirements (as opposed to compliance requirements) into security technology and service actions simply cannot happen. In that circumstance, digital trust cannot happen.



Figure 14 is one example of the difference such a translation can make. On the left side of the figure is an example of the typical goals (requirements) assigned to carrier security teams. All of those requirements are compliance oriented and (almost) independent of the functional purpose of the system. On the other hand, the right hand side of Figure 14 shows a translation of functional requirements (in this case for a field force support system) that expresses answers to the essential digital trust question, “What will be different about the business with digital trust?” The translations come not from the typical security requirements, but rather are translations of the business objectives of the intended system. The obligation for compliance is stated for convenience in one sweeping assignment, and digital trust provides that result as one outcome of the value-generation pursuit. Two measurements are taken as the system is completed: (1) measurement of the payoff captured, and (2) measurement of the difference (or degree) of compliance.



Payoff Potential Remains

“Payoffs missed” does not mean “payoffs lost.” The systems that were explored still contain the seeds of digital trust dividends that remain to be captured. Figure 13 provided one example of how digital trust could alter the value potential to the enterprise for one of the (converged) systems. The good news is that *all* of the specific systems examined had just such a potential. And, the extended logic would indicate that all systems *like* those examined would have equivalent latent digital trust payoffs, as well. That is more good news for the life and annuity industry at large. Furthermore, the security teams appear well trained and sufficiently experienced to take advantage of digital trust principles and practices.



But, these potential payoffs are not retrievable by the industry at large. They must be pursued and captured by individual carriers against their own business objectives, through their own specific systems.

Furthermore, beyond the immediate tactical opportunity to apply some digital trust principles and practices to systems already deployed lies the strategic opportunity to adopt digital trust as an enterprise (security) operating method, and pursue value creation through security technologies and services as a natural and ongoing practice. That strategic adjustment need not be made all at once. In fact, the results of the effort described in Part 2: Digital Trust Projection (see Figure 5) revealed that just two steps were needed to begin that strategic adjustment, even while seeking more immediate digital trust payoffs from systems already in place.

Part 2 — Digital Trust Projection

Even while sample systems were being analyzed for evidence of current digital trust practices and technology uses, those same systems were being “projected” into additional potential value creation by applying the fundamental digital trust translation question for security: “How will the business be different with digital trust?” (See Figure 14.) And, while the analysis effort was actually being done against two different value objectives, the results of the projection work delivered nearly the same potential business-impact avenues for payoff, regardless of which value objective was being used. In other words, the *business objectives* that seemed to offer the best payoff potential with digital trust were almost the same across both value objectives. If automated (security) technologies or services could be applied to those objectives, then value would result — and, by the way, risk exposure would be reduced. That’s precisely digital trust!

Initial Business-Impact Areas

After the initial digital trust projection work, eight business-impact areas were identified as avenues for digital trust (and potential payoffs). This first set of eight is shown in Figure 15. Other avenues would no doubt be added once specific carrier system implementations (as opposed to the converged characterizations used on behalf of the industry) were exclusively examined.

	Customer service and distribution management	Organic growth and competitive advantage
1. Move beyond current client base	✓	✓
2. Attract and motivate agents and customers with “client-centric” online experience	✓	✓
3. Produce simple/single sign-on across applications	✓	✓
4. Support captive and independent agent field forces with the same IT infrastructure	✓	✓
5. Promote use of “consumer IT” in agent field force	✓	✓
6. Extend agent sessions with clients (virtually) beyond the actual face-to-face or ear-to-ear session	✓	✓
7. Provide for full electronic completion of applications/contracts with or without agent presence (including signatures)	✓	✓
8. Eliminate need for clients to have “special equipment” to complete forms and/or check on account status		✓

Figure 15. Potential Business-Impact Areas for Digital Trust



Seven of the first eight areas that were identified, applied across both value objectives. Only the business impact area dealing with eliminating special equipments for clients to complete forms was isolated to the “organic growth and competitive advantage” value objective. And, even that one could, under a broad interpretation, logically be extrapolated to support the “customer service and distribution management” value objective.

“What If” Scenarios for Digital Trust Technology Projections

Once the initial business-impact areas were chosen, digital trust technology “what if” scenarios were advanced to see whether value would result if the “what if” condition could be satisfied. Each scenario is expressed in terms of security technology features, or functions, or evidence factors. Ultimately this question is answered by individual enterprises (in this case, carriers) who make the ultimate decision about whether or not enterprise value would be generated. This decision is greatly influenced by the digital trust reality that *risk reduction is a natural consequence* of the value creation agenda. However, notwithstanding this digital trust reality, not all “what if” scenarios bring digital trust to every enterprise.

Initial Scenarios

Figures 16 and 17 provide *initial* lists of “what if” scenarios for projection over each of the two value objectives. These scenarios were selected based on the converged characterizations of the industry used in this study. Other additional or replacement scenarios would be generated for an individual carrier depending on that carrier’s specific business and technology circumstances.

These initial “what if” scenarios are particularly attractive because, in each case, “we can!” All of these scenarios have a digital trust technology response — i.e., a corresponding security-relevant technology that has shown itself capable of generating value. Nearly all have already demonstrated that value capture.

What if we could ... ?

1. Provide an “agent single sign-on (SSO)” capability for captive agents across all producer applications?
2. Create a federated identity scheme so that independent agents could automatically be admitted to the application base without having to get corporate user ID’s from every company?
3. Use federated identity scheme to generate electronic signatures as well?
4. Use another (simpler) qualifying technique to capture electronic signatures with and without automated workflow? ... and without using signature tablets?!
5. Make any agent PC (captive or independent) able to host agent apps in accordance with company rules?
6. Empower applicants to prepare data without an agent being literally present?
7. Provide a legally enforceable “certified/registered” e-mail capability that does NOT require recipients to have any special software or hardware on their own systems?

... Knowing that risk reduction is a natural consequence ...

Questions for Each Carrier

- How would the business be different?
- What could the payoffs be?

PC2003-1432-015e, 3/6/09

Figure 16. Initial “What If We Could ...?” List for Customer Service and Distribution Management



These scenarios were selected from digital trust applications in a variety of industries. Many were chosen based on application and payoff in industries that are similar to life and annuity industry business objectives and operations. In some cases, the examples are carriers themselves or their agents. For instance, the RPost registered e-mail service (see item 7 in Figure 16 and item 6 in Figure 17) is already being used by Aon³³ and brokerages in the Assurex Global Partners network,³⁴ and is endorsed by the Council of Insurance Agents and Brokers (CIAB).³⁵

What if we could ... ?

1. Extend the enrollment sessions to the enrollee's own office or home?
2. Have enrollment apps work on the enrollee's own portable device?
3. Provide subsequent related/relevant subscriber feeds to enrollees based on their own interests as expressed during enrollment sessions?
4. Have secure virtual agents/avatars guide prospects through the alternatives and enrollment steps?
5. Make electronic signatures possible in enrollment sessions (or extended enrollment sessions)?
6. Provide a legally enforceable "certified/registered" e-mail capability that does NOT require recipients to have any special software or hardware on their own systems?

... Knowing that risk reduction is a natural consequence ...

Questions for Each Carrier

- How would the business be different?
- What could the payoffs be?

PC2003-1432-016d, 3/6/09

Figure 17. Initial "What If We Could ...?" List for Organic Growth and Competitive Advantage

Similarly, ING Canada is already deploying a secure e-mail system from Voltage Security that uses zero-download identity-based encryption to send secure e-mail to independent insurance brokers and business partners.³⁶ In other cases, the exemplars are from industries with comparable regulatory and/or business models (e.g., banks and credit unions, pharmaceuticals).³⁷ In still others, the scenarios are extrapolated from unrelated industries into a life and annuity context. A good example here is the use of "bots" of all types — e.g., virtual agents and avatars — to deliver speedy, efficient, tireless and *absolutely compliant* service support, advice, and follow-up in such industries as health care, safety, reservations, customer service, human resources, law enforcement and student registration.³⁸ (See item 6 in Figure 16 and item 4 in Figure 17.)

Using the Digital Trust Scenarios for Value Projection

What others have done is interesting. But, what the life and annuity carriers *can do* is the real attraction here. The examples of how others have used digital trust technologies to capture payoffs are helpful, but the action for each carrier is to answer the two enterprise questions of Figure 16 and 17:

1. How will the *business* be different with digital trust?
2. What could the payoffs be?

Whenever the answers respond to the value objectives, carriers can apply digital trust technology to generate value for their own enterprise. Furthermore, if the experience of others is representative, some of the potential payoffs are substantial. On the other hand, if the two enterprise questions for digital trust cannot be answered in terms that respond to the value objectives, then there is likely no opportunity in that projection for digital trust value.



Two of the “what if” digital trust technology scenarios are duplicated in Figures 16 and 17. (Items 5 and 6 of Figure 17 are essentially the same as items 4 and 7 of Figure 16.) This circumstance suggests that these digital trust technologies could deliver a double payoff by contributing to both value objectives. However, even in this case, the enterprise questions must be answered positively.

In this study, the “what if ...” digital trust projection questions were asked, but not specifically answered by the participants. Each reader is invited to respond to these scenarios on behalf of their own enterprise in light of each of the two value objectives. However, based on the converged characterizations of systems used in this study, the digital trust projection against the “what if” scenarios in Figures 16 and 17 would appear to have broad applicability and success in generating digital trust dividends for an enterprise generally representative of the carrier population within the ACLI.



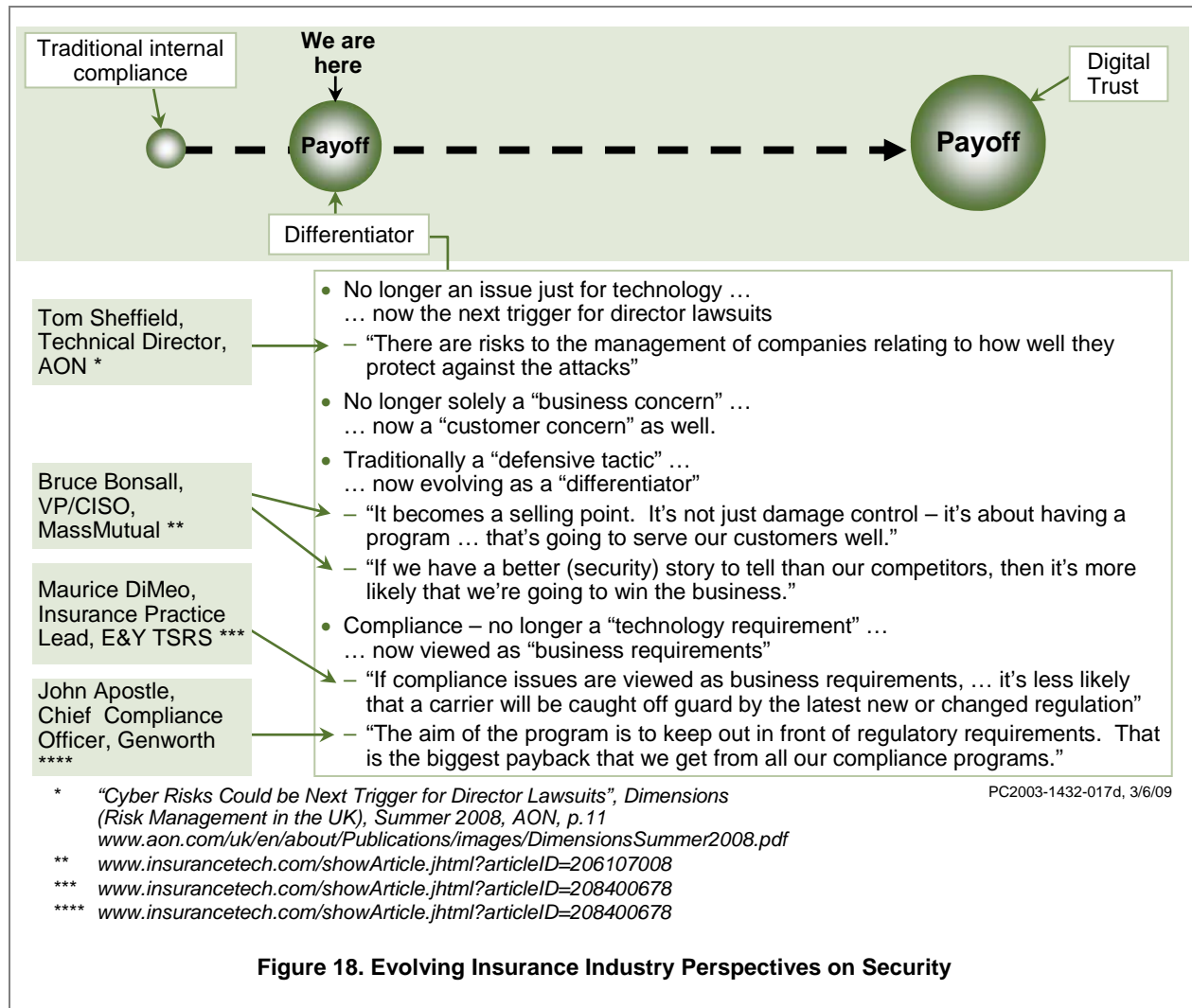
CONCLUSIONS AND RECOMMENDATIONS

Study Observations and Conclusions

“So near ... and yet so far.” The results of the study are tantalizing. No direct evidence of digital trust strategy, practices or principles was discovered, but the most typical systems already deployed by life and annuity firms seem “ripe” with opportunity for digital trust targeted at the two value objectives. The industry is poised for payoffs with digital trust. There are three main observations supporting this conclusion:

1. *Life and annuity industry security teams are doing a good job against their assigned objectives.* Compliance with a host of regulatory mandates and policy directives is the system and process mission typically given to these teams. Their activity is normally applied as part of a checklist of approval before systems can be deployed. Working in this “gatekeeper” model of operation, the industry security teams evaluate and test systems and system components against compliance criteria. Ultimately, systems are altered and refined in response to security team findings so that compliance standards are satisfied, and the systems can then be deployed. Even though cost reduction did appear as a target for security, from time to time, *compliance* is the primary (and sometimes only) measure of success.
2. *No security teams were found to be in the lead for architecture or system development.* We did find some creative and clever suggestions and recommendations from security staff in pursuit of compliance, but rarely was there opportunity for security teams to introduce functional alterations or expansion. In most cases, a security team presence was brought in only after much of the design definition and many of the development decisions had already been made. Still, the deployed systems are fertile ground for digital trust. The example in Figure 13 is just one illustration of how each of the 13 initial digital trust technology scenario projections (from Figures 16 and 17) could apply. There appear to be many good places to start.
3. *Industry security leadership is interested in “going further” and was curious about the principles and realities of digital trust.* During interviews, security representatives responded that they were anxious to be able to “tell a good story” and to use security as a “business advantage” rather than “a necessary evil.” While the emphasis is still clearly compliance, Figure 18 suggests that the outlook is evolving. As evidenced by the series of quotes from insurance industry specialists, security has moved from an asterisk issue of technology to become :
 - Board-level business issue
 - Customer issue
 - “Differentiator” for companies attempting to gain competitive advantage

Digital trust is the way to accelerate this inevitable evolution past the point of enterprise differentiation and on to real business payoffs.



Recommendations

Digital trust is available for the life and annuity industry. Furthermore, the industry has already invested in systems that are ready sources of value through digital trust practices and technologies.

Unfortunately, capturing value potential with digital trust is not automatic, no matter how much that value is wanted. Without some changes in security organization, security team composition, IT risk governance, security project definition and the ways in which security analysis and technology choices are made, digital trust payoffs will not occur.

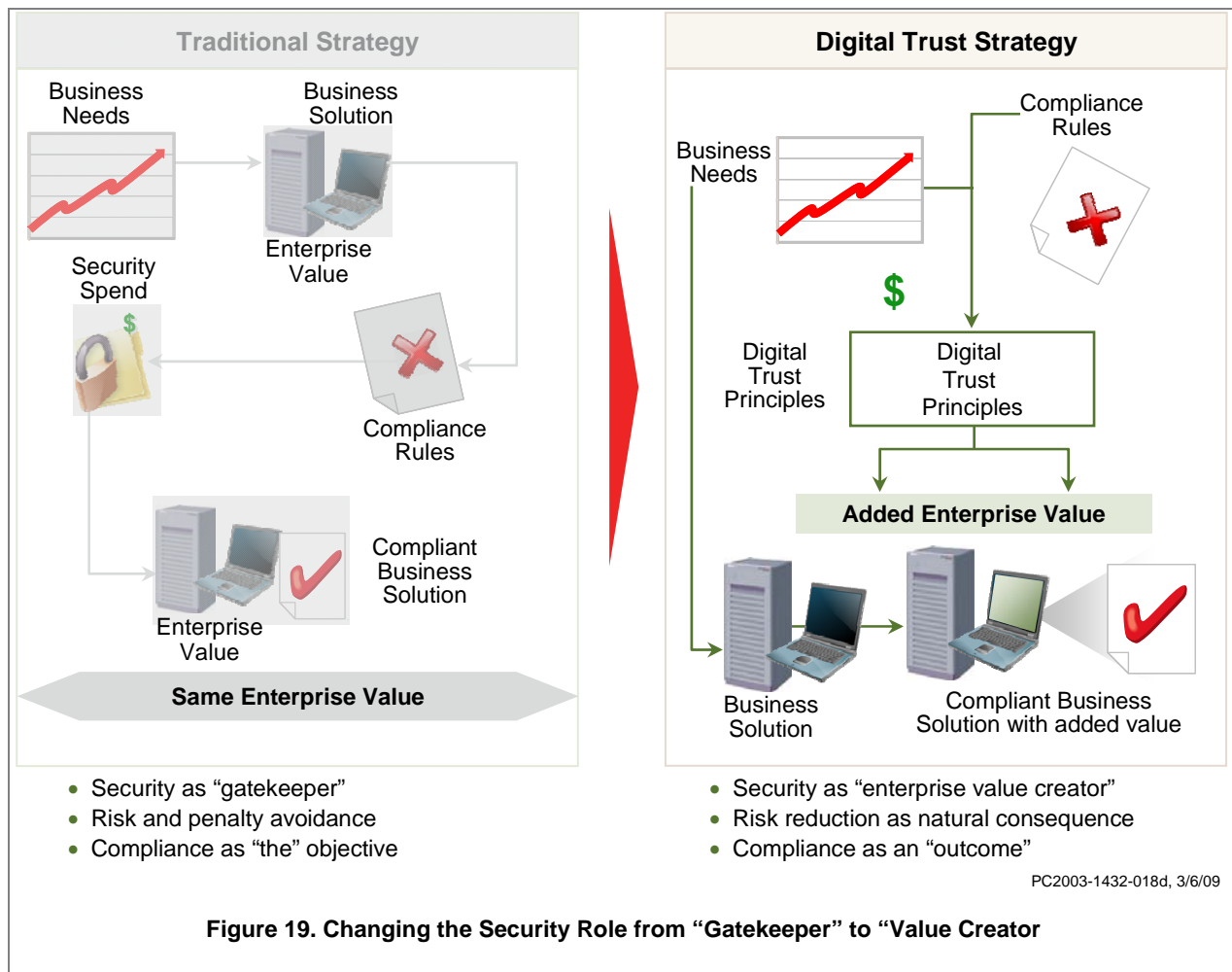
However, the evolution to a digital trust strategy need not be done all at once. In fact, this study recommends taking just two near-term actions right now to begin seeking and capturing digital trust payoffs from systems already deployed or in the design process. The ultimate decision to evolve to an enterprise digital trust strategy can be made later, with the benefit of experience gained in applying these two actions. Once confident with digital trust, an enterprise can build on these two initial steps and complete the metamorphosis to a full digital trust enterprise.



Action 1: Alter the IT Risk Governance Model to Support Digital Trust

Alter the IT risk governance model to include enterprise value creation as an objective. For life and annuity companies, this means changing the traditional role of security as “gatekeeper” to one of “value creator.”

Figure 19 illustrates the impact of the change from a traditional “gatekeeper” strategy to a digital trust strategy. Under the gatekeeper model, the business needs that underlie system development are often obscured. Many times, even the system solution is hazy until it is declared ready for the compliance checkoff step that includes a security approval (the security gatekeeping action).



Once introduced to the effort, the security team spends time and effort to evaluate the system against a set of compliance rules, and either passes the system to its next deployment checkoff, or sends it back to development for more adjustment to satisfy compliance requirements. Compliance is the objective, and avoidance of penalties due to non-compliance is the measuring stick. Even if the security team does its job perfectly, *no additional enterprise value is created.*

On the other hand, a digital trust strategy connects the security teams directly to the business needs as well as the compliance rules. Security efforts are now directed by a “business translation” of



objectives (see Figure 14) rather than repeating the same functional compliance requirements over and over, regardless of the system's underlying business targets. Role descriptions for security team members now include value creation as a responsibility. New value created through an application of digital trust practices, principles and technology choices is now the objective. Risk exposure is reduced and compliance is improved as one (natural) outcome of the digital trust practice. In this strategy there are two measuring sticks:

1. The kind and amount of new value created through digital trust.
2. The difference in risk exposure and compliance from beginning to end.

This step moves IT security teams to change the way projects are approached and priorities are established. It also changes the way technologies are chosen. When done correctly, the security team has *added new value to the enterprise*, while still achieving the compliance outcome as well. Figure 13 illustrates the difference in outcome between the traditional gatekeeper model and a digital trust strategy.

Action 2: Bring Digital Trust to Current Systems

Apply a digital trust projection to already deployed systems. The systems profiled by the converged characteristic representations in Figures 9 through 12 appear ready for digital trust. These systems represent not only a path to capture early payoffs on well-understood deployments, but also an ideal training ground for learning digital trust practices.

Figures 16 and 17 provide an initial list of 13 “what if” scenarios that are available for a digital trust projection to typical (currently deployed) systems. These initial projections concentrate first on those value creation avenues that have already proven so successful in other industries and that seem directly relevant to the systems and value objectives targeted in this study.⁴ The results of this study indicate that payoffs of similar magnitudes should be available to the insurance and annuity industry.

Becoming a Digital Trust Enterprise

The two actions recommended in this study are the first steps toward an enterprise digital trust strategy. They are important steps that affect the ways in which security teams are formed and operated, and the ways in which security requirements, features, functions and technologies are identified, examined and chosen.

However, there are other actions required to take full and sustained advantage of the realities of digital trust. Figure 20 maps the entire evolutionary path to a digital trust strategy. Those items shown in red indicate where the two recommended actions are located in the full path. The two steps shrouded in the “transition stage” oval need only be done once to account for all promising current deployments. After that, the digital trust strategy accounts for those actions as new business needs (and corresponding systems) are defined.

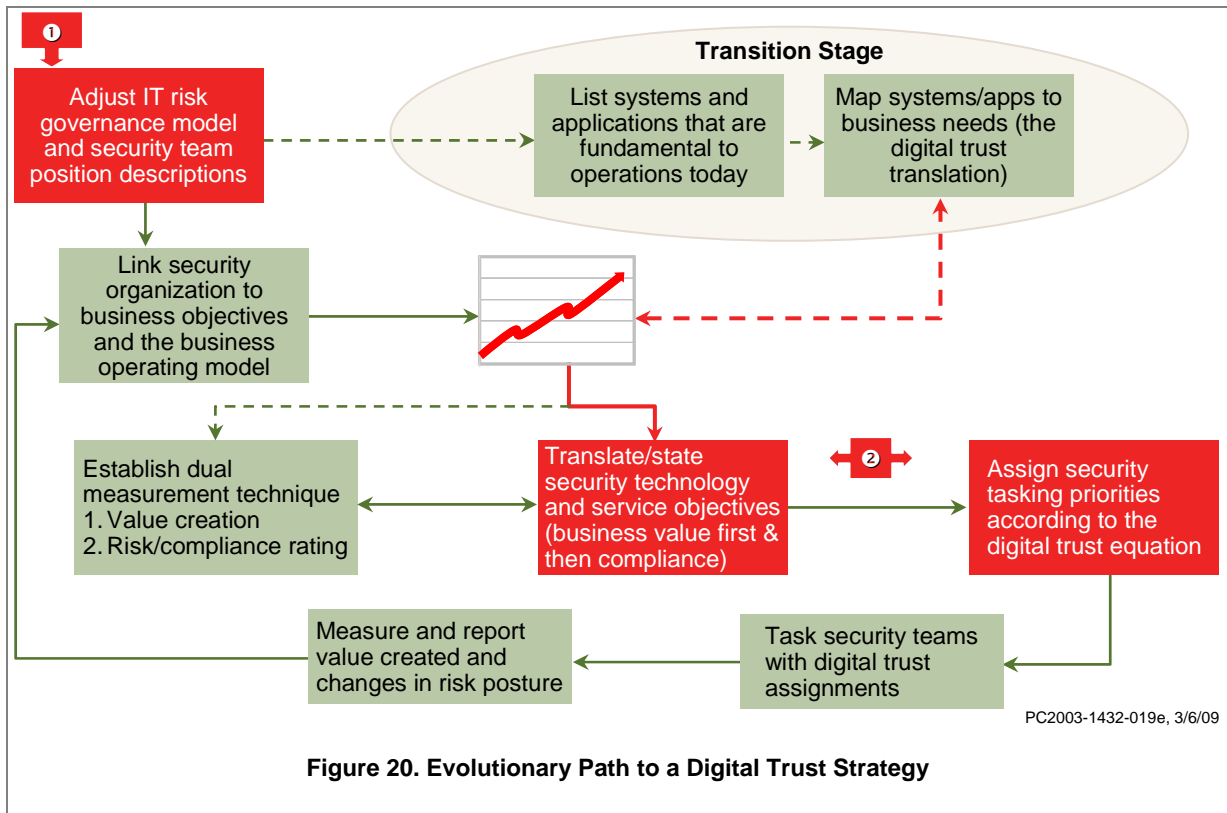


Figure 20. Evolutionary Path to a Digital Trust Strategy

The two recommended actions can move an enterprise to digital trust value capture for systems already known and operating. However, if the full path is followed, that enterprise value capture is no longer seen as a special event. Rather, it becomes a *strategic expectation*. That marks the start of a *digital trust enterprise*. And, that's real "digital trust for life."



APPENDIX A CSC DIGITAL TRUST RESEARCH PROGRAM OVERVIEW

(Extracted From Volume 8, Epilogue and Strategic Roadmap)

Shake Hands with the Digital Enterprise

“Digital trust” is how we shake hands with the digital enterprise. This is the ultimate reality of the research program recently concluded by CSC.³ Using the metaphor of a handshake, this research program explores the ability to *create value* with security services and technologies, rather than attempting only to do an incrementally better job of protecting the value that already exists. Digital trust is technology’s contribution to the total complement of enterprise and transaction trust.



This initial exploration of digital trust confirmed the reality of power and payoff with security technology and services when used in a digital trust strategy. That strategy was shown to amplify the full harmony of all contributions to enterprise trust, and deliver real new and direct value. Digital trust as defined here was shown to be more than just a concept or a notion or an approach or even a point of view. Digital trust is the use of technology:

- Developed and applied in the name of security
- With the intent of creating value for the enterprise
- Knowing that information risk reduction will come, as well

The report covering this first exploration spans eight volumes and runs through all major contemporary issues in security, weaves through some spectacular next-generation technology and concepts of operation, looks at the most difficult terrain of uncontrollable threats, and even examines the gauges and meters that enterprises use to measure the “weight” of digital trust and its effect on their “enterprise speed to value.”

As illustrated in Figure A-1, the volumes form a continuum of research exploration and results. Within each volume are descriptions of digital trust technologies being used and payoffs being generated. The variety of ways in which real additional value is being created by enterprise applications of digital trust is remarkable in both its breadth and depth. Digital trust happens globally and in every kind of industry. Payoffs are created and captured with applications of digital trust technologies both within a single key area, and, even more powerfully, across multiple key areas. The first journey on the trail of digital trust is done. The results are in, and the evidence is complete and convincing.

Digital trust is a security technology reality.



Strategic Conclusions

The journey along the trail of digital trust delivered four strategic conclusions:³⁹

1. *Digital trust is real.* Enterprise value can be created with security technology and services. Investing only to gain vague reductions in the risk of loss to existing value is no longer the only option.
2. *Aim high and first with a digital trust strategy to get the payoffs.* The value creation payoffs of digital trust are most often collected when targeted as an objective of the security task. The enterprise must “aim” for them. Furthermore, a digital trust strategy for enterprise value creation almost always brings information risk management (reduction in risk of loss) as a natural consequence. On the other hand, focusing on information risk management does not usually grow to a digital trust result.
3. *Security governance structures prevent digital trust strategies from being used more widely.* Security authorities are not often given credit for value enhancement. The traditional rewards are simply for reduction in the risk of loss. Consequently, security authorities lack practice and incentive for value creation. Digital trust is a learned behavior and must be taught for strategic viewpoint and technology selection and application.
4. *Evidence-based confidence generation is the pervasive technology shortfall.* Technologies are being created and applied for digital trust results. Digital trust payoffs are delayed and reduced when digital trust claims (announced as features and functions) lack credible digital trust confirmations and evidence (i.e., come up short on transparency and assurance).

The conclusions are powerful, and they reaffirm the use of digital trust as the basis for a security technology strategy that enhances business value while at the same time tends to important information risks everywhere in the modern digital enterprise.⁴⁰

What Now?

But, like most good explorations, there are two other useful outcomes beyond our firsthand encounters with digital trust:



1. *We can now make a sketch of a digital trust strategic roadmap for others to follow. We have seen enough to post fundamental digital trust directions and signposts that others can follow to accelerate their own value creation and generate the largest possible payoffs, without having to explore every pathway for themselves.*⁴
2. *We have a list of intriguing paths we saw but did not explore. We noticed trails that hinted at more ways to create and capture value with digital trust. As powerful as the realities of digital trust are today, there may be even more ways (better ways?) to capitalize on digital trust that are waiting for us just around the (digital) bend. Now that we know the “lay of the land,” other targeted explorations may be even more attractive and have the potential to be even more productive.*

With these two additional outcomes in hand, we can not only make a sketch of the digital trust paths we *did* explore, but we can also point the way to some potential digital trust paths that *ought to be* explored, as well.

Unexamined Realities

Two roads not traveled in the first digital trust exploration form the core of the next-stage digital trust agenda. They involve further inspection of additional potential realities (payoffs) for digital trust and an examination of whether industry-specific techniques exist that can help speed the design and capture of digital trust payoffs.

1. *Does the pursuit and application (and payoff) of digital trust differ depending on the industry segment? Is a digital trust strategy easier to apply in certain industries? Do some digital trust technologies only work in certain industries? How can we best identify and deploy digital trust technologies, given that we have specific industry needs and objectives known to us?*
2. *Do the other realities of the full harmony of trust apply specifically to digital trust as well? For example, the Digital Trust study fully explored the application of Stephen Covey’s reality, “Nothing is as fast as the speed of trust,”⁴¹ to technology’s contribution to trust — i.e., digital trust. Now, we know that “Nothing is as fast as the speed of *digital* trust” is reality as well. But there are other important trust realities that could make digital trust even more valuable. For example, Covey also declares that “nothing is as profitable as the economics of trust”.⁴² Wouldn’t that be a powerful conclusion for digital trust, too?!*

¹ From CSC/ACLI research paper, “Economic Impact of an Optional Federal Charter on the Life Insurance Industry,” published November 2005. Available at http://assets1.csc.com/financial_services/downloads/ACLIFExecSumm.pdf.

² From Celent Communications, “The Virtuous Cycle of Compliance and IT?”, November 2004, p.3. Available at www.celent.com.

³ The entire *Digital Trust* series can be found at <http://www.csc.com/aboutus/leadingedgeforum/mds/mds436/844.shtml>

Volume 1 — Digital Trust: Shaking Hands with the Digital Enterprise
 Volume 2 — Identity Management: Digitizing Your DNA
 Volume 3 — Intellectual Property Protection: Minding Your Mind Power
 Volume 4 — Compliance Management: The Business of Keeping the Business in Business
 Volume 5 — Liquid Security: Digital Trust When Time, Place and Platform Don’t Matter



Volume 6 — eThreats and Countermeasures: Just When You Thought It Was Safe to Go Out
Volume 7 — Transparency and Assurance: Putting a Measure on Digital Trust
Volume 8 — Epilogue and Strategic Roadmap

⁴ Volume 8 in the *Digital Trust* series offers a roadmap suggesting technologies that delivered the greatest payoffs (or potential payoffs) throughout the research study. These are the technologies that should be examined first by those organizations beginning their evolution to a digital trust enterprise. See “Digital Trust: Epilogue and Strategic Roadmap,” Volume 8 in the *Digital Trust* series, “What’s Next? Roadmap and the Rest of the Story,” pp.18–20.

www.csc.com/aboutus/leadingedgeforum/knowledgeibrary/uploads/LEF_2008DigitalTrustVol8.pdf

⁵ This is taken from the penultimate sentence in the concluding paragraphs of the final volume of the *Digital Trust* series. See “Digital Trust: Epilogue and Strategic Roadmap,” Volume 8 in the *Digital Trust* series, “Finale,” p.26.

www.csc.com/aboutus/leadingedgeforum/knowledgeibrary/uploads/LEF_2008DigitalTrustVol8.pdf.

⁶ See footnote 3.

⁷ For a more complete description of the four strategic conclusions of the first Digital Trust study, see “Digital Trust: Epilogue and Strategic Roadmap,” Volume 8 in the *Digital Trust* series, “The Results Are In,” p.3.

www.csc.com/aboutus/leadingedgeforum/knowledgeibrary/uploads/LEF_2008DigitalTrustVol8.pdf

⁸ With only two exceptions, all the formulas on which all risk management, including information risk management, are based were determined and proved during the Renaissance. The formula typically used as the foundation for all contemporary information risk management practices can be found in “Digital Trust: Shaking Hands with the Digital Enterprise,” Volume 1 in the *Digital Trust* series, Figure 1-6, “Traditional Information Risk Management Formula,” p.6.

www.csc.com/aboutus/leadingedgeforum/knowledgeibrary/uploads/LEFReports2007_DigitalTrustVol1.pdf

⁹ See the second strategic conclusion in “Digital Trust: Epilogue and Strategic Roadmap,” Volume 8 in the *Digital Trust* series, “The Results Are In”, p.3.

www.csc.com/aboutus/leadingedgeforum/knowledgeibrary/uploads/LEF_2008DigitalTrustVol8.pdf

¹⁰ For example, see the experience of Xerox and its use of Common Criteria certification in “Transparency and Assurance: Putting a Measure on Digital Trust,” Volume 7 in the *Digital Trust* series, “Certified Payoffs,” p.19.

www.csc.com/aboutus/leadingedgeforum/knowledgeibrary/uploads/LEF_2008DigitalTrustVol7.pdf

¹¹ See the effect of trustmarks for online shopping in “Transparency and Assurance: Putting a Measure on Digital Trust,” Volume 7 in the *Digital Trust* series, “Digital Trust Payoff in Click Stores,” pp.11–14.

www.csc.com/aboutus/leadingedgeforum/knowledgeibrary/uploads/LEF_2008DigitalTrustVol7.pdf

¹² See examples of penalties for loss of intellectual property in “Intellectual Property Protection: Minding Your Mind Power,” Volume 3 in the *Digital Trust* series, “The Cost of Digital Trust Deficits for IP,” pp. 6-8.

www.csc.com/aboutus/leadingedgeforum/knowledgeibrary/uploads/LEF_2007DigitalTrustVol3.pdf

¹³ www.customerrespect.com/default.asp?hdnFilename=bwlifeq308.htm

¹⁴ <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>

¹⁵ There are many descriptions of the TJX privacy data breach, covering everything from a timeline to vulnerabilities, culprits, ultimate costs and restoration efforts. See

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9014782> for a good beginning overview. Volume 8 of the *Digital Trust* series (www.csc.com/aboutus/leadingedgeforum/knowledgeibrary/uploads/LEF_2008DigitalTrustVol8.pdf)



contains seven additional references that follow the TJX breach saga to its conclusion, including ultimate restoration of stock price and consumer confidence. See pp.12–13.

¹⁶ See the tally of penalties to TJX in “Digital Trust: Epilogue and Strategic Roadmap,” Volume 8 in the *Digital Trust* series, “Where (and How) Are They Now?” pp.12–13.
www.csc.com/aboutus/leadingedgeforum/knowledgelibrary/uploads/LEF_2008DigitalTrustVol8.pdf

¹⁷ “Ponemon Study Shows Data Breach Costs Continue to Rise,” press release, 28 November 2007, www.ponemon.org/press/PR_Ponemon_2007-COB_071126_F.pdf. The entire study report, “2007 Annual Study: U.S. Cost of a Data Breach,” is available at www.vontu.com/downloads/ponemon_07.asp (registration required).

¹⁸ Reported in “Key Performance Indicators,” Softchoice Security Advisor, 2007 Technology Buying Guide, p.13, http://www.softchoice.com/advisor/pdf/Security_Advisor_Web.pdf. Original data from “The Security of Information: A Strategic Approach to Current Topics and Trends,” EMA Market Research Study, September 2006, http://www.emausa.com/research/ema_product.php?product=5000_1193

¹⁹ “A.R.C. Morgan: More than 60 Percent of CFOs Resign or Are Pushed when a Material Weakness is Disclosed,” *DM Review*, 7 December 2004, http://www.dmreview.com/article_sub.cfm?articleID=1015148

²⁰ An inevitable increase and alteration in regulation has become “conventional wisdom.” See, for example, the predictions by IDG News Service in “New Regulations will soon swell IT workloads,” *InfoWorld*, 12 November 2008, www.infoworld.com/article/08/11/12/46FE-tech-new-regulation_1.html

²¹ See the two goals listed in this report under “The Beginning” on p.7.

²² www.insurancenetworking.com/news/insurance_technology_portals_web_sites11060-1.html.

²³ In an October 2008 statement by CSC executives representing the Life and Annuity practice of CSC's Financial Services Sector.

²⁴ For instance, there are many online sites that offer “instant quotes” for term life. Some even offer to provide a quote, complete an online application and initiate coverage (including printing the policy itself), all in the same session. See, for example, www.netcoverage.com/default.aspx?afid=9872.

²⁵ www.serff.org/about.htm

²⁶ One of the most publicized examples of this type of customer support platform (targeting organic growth and competitive advantage) is the MassMutual e4 system. See www.informationweek.com/story/showArticle.jhtml?articleID=192700123 and www.insurancenetworking.com/news/11072-1.html for an introduction and some updated business results.

²⁷ A good discussion of the enterprise evolution of automated support for these end-to-end process objectives can be found in an early case study of events and developments at Amica Life. See www.fiservinsurance.com/downloads/INN_AmicaArticle.pdf

²⁸ Example back office staff reduction savings are based on a 25 September 2008 Digital Trust interview with an executive from a major health and life company.

²⁹ “Liquid security” is a category of digital trust technology and use as described in Volume 5 of the *Digital Trust* series, “Liquid Security: Digital Trust When Time, Place and Platform Don't Matter,” 25 September 2007, www.csc.com/aboutus/leadingedgeforum/knowledgelibrary/uploads/LEF_2007DigitalTrustVol5.pdf

³⁰ See “The Rise of Consumer IT,” <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=281783>, and



“Gartner Says Consumerization Will Be Most Significant Trend Affecting IT During Next 10 Years,” http://www.gartner.com/press_releases/asset_138285_11.html, for an introduction to the value potential of consumers using their own IT for enterprise (corporate) assignments and business.

³¹ See *Harnessing Web 2.0: Enterprise Strategies for Living on the Web*, 3 April 2007, <http://www.leadingedgeforum.com/library/publicationdetail.aspx?id=1128>

³² See “Digital Trust: Epilogue and Strategic Roadmap,” Volume 8 in the *Digital Trust* series, “What’s Next? Roadmap and the Rest of the Story,” pp.18–21. www.csc.com/aboutus/leadingedgeforum/knowledgelibrary/uploads/LEF_2008DigitalTrustVol8.pdf

³³ www.riskandinsurance.com/story.jsp?storyId=141399827 and at www.rpost.com/site/press/news/2008-11_Risk_insurance_mag.pdf

³⁴ www.rpost.com/site/press/news/200807_Brokers.htm

³⁵ www.rpost.com/site/press/news/200702_ciab.htm

³⁶ www.itbusiness.ca/it/client/en/Home/News.asp?id=41982

³⁷ For example, electronic signature services from AlphaTrust and DocuSign are used by many enterprises, highly regulated and otherwise. Such enterprises as BearingPoint, CareFirst and the Federal Aviation Administration use the AlphaTrust PRONTO e-Signature service (www.alphatrust.com/projects/), while Expedia, Yamaha and Great Lakes Educational Loan Services use an equivalent electronic signature service from DocuSign (www.docusign.com/customers/success_stories/). Neither requires special devices or even special client software! Meanwhile, Pfizer has multiplied its value capture by combining digital trust technologies in federated identity and electronic signing using technology from the SAFE bridge certificate authority and TriCipher (www.safe-biopharma.org/infocenter/b-Pfizer-CaseStudy-Summary.pdf). CSC’s own banking software now leverages the SignatureOne Ceremony Server signature software from Communication Intelligence Corporation (CIC) (www.cic.com/Apps/PRDetails.aspx?id=295). AIG, Prudential and Nationwide (UK) have already included CIC technology in their applications.

³⁸ See http://fora.tv/2008/08/08/Daniel_Suarez_Daemon_Bot-Mediated_Reality for a good overview of current bot technology use.

³⁹ For a more complete description of the four strategic conclusions of the Digital Trust study, see “Digital Trust: Epilogue and Strategic Roadmap,” Volume 8 in the *Digital Trust* series, “The Results Are In”, p.3. www.csc.com/aboutus/leadingedgeforum/knowledgelibrary/uploads/LEF_2008DigitalTrustVol8.pdf

⁴⁰ “Digital Trust: Shaking Hands with the Digital Enterprise,” Volume 1 in the *Digital Trust* series, “The Beginning of Digital Trust,” pp.2–3. www.csc.com/aboutus/leadingedgeforum/knowledgelibrary/uploads/LEFReports2007_DigitalTrustVol1.pdf

⁴¹ Stephen M.R. Covey, *The Speed of Trust* (New York: Simon & Schuster, 2006), pp.3–26.

⁴² *Ibid*, p.285.



ACKNOWLEDGEMENTS

Ron Knode — Principal Author



Ron Knode is a director in CSC's Global Security Solutions business unit and leads the "Digital Trust" research program in CSC's "innovation think tank," the Leading Edge Forum. Mr. Knode has been primary researcher and author for the "Digital Trust" program, which explores an enterprise's ability to create new value with security services and technologies (the program's eight-volume report is available on csc.com.) Prior to this, he was responsible for all aspects of the end-to-end security solutions that support CSC's clients worldwide.

Coming to CSC after 7 years in the Naval Security Group and executive roles at Logicon and ARC, Mr. Knode served as program manager of the DISA Infosec TSC contract. During that same period, he also served as Lead Information Risk Manager for JPMorgan and DuPont, and established CSC's IRM outsourcing service center. He was CSC's representative to the President's National Security Telecommunications Advisory Council (NSTAC) and is on the Board of Advisors for the National Security Foundation-funded CyberWatch security center.

Mr. Knode has served on the National Defense University faculty, currently teaches at Towson University and is in high demand as a lecturer and speaker. Mr. Knode holds bachelor's and master's degrees in mathematics from the U.S. Naval Academy and the U.S. Naval Postgraduate School and has completed doctoral coursework in computer science at the University of Maryland. He has been a Certified Information Security Manager and is a Black Belt in Six Sigma quality improvement processes.

Bob McDonald — Author

Bob McDonald is a principal consultant with CSC's Financial Services Group and specializes in strategic application of IT for business transformation within the life and annuity industry. Mr. McDonald has extensive experience in analysis of life and annuity business operations, including product development, distribution, new business and client service. He currently focuses on developing technology plans that leverage current and emerging technology to meet clients' strategic business goals. Mr. McDonald offers over 20 years of experience in the definition, deployment and operational management of complex information systems solutions. He is a regular contributor to the ACLI and has authored publications on the Optional Federal Charter and on annuities and retirement security. He holds graduate degrees in engineering and economics from Rice University.



Greg Stites — Author



Greg Stites is a senior compliance officer with CSC's Financial Services Group and works primarily with its licensed third party insurance administrator (TPA) organization. Mr. Stites oversees the compliance department for CSC's life, health insurance and annuity product TPA subsidiaries. He maintains CSC's subsidiary TPA licensure in all state jurisdictions, and interfaces with state and federal regulatory authorities on compliance matters. Mr. Stites offers over 20 years of experience specializing in current and pending state and federal regulation/legislation, case law and public/industry responses to insurance regulatory compliance issues. Mr. Stites holds an undergraduate degree in industrial engineering as well as a JD degree. He has been a practicing attorney for 32 years.



SPECIAL THANKS

CSC and the ACLI would like to acknowledge those who have contributed to this report. Many people directed us to policy documents, system descriptions, regulatory materials and reference items of all types. However, some were extra generous with their time and attention. To these, we offer special thanks.

- The staff of the American Council of Life Insurers (ACLI)
- Eunice Holmes, Allstate (American Heritage Life)
- Bruce Bonsall, CISO, Mass Mutual

**North American Public Sector**

3170 Fairview Park Drive
Falls Church, VA 22042
+1.703.876.1000

Worldwide CSC Headquarters**The Americas**

3170 Fairview Park Drive
Falls Church, Virginia 22042
United States
+1.703.876.1000

Europe, Middle East, Africa

Royal Pavilion
Wellesley Road
Aldershot, Hampshire GU11 1PZ
United Kingdom
+44(0)1252.534000

Australia

26 Talavera Road
Macquarie Park, NSW 2113
Australia
+61(0)29034.3000

Asia

139 Cecil Street
#08-00 Cecil House
Singapore 069539
Republic of Singapore
+65.6221.9095

About CSC

The mission of CSC is to be a global leader in providing technology-enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.

CSC makes a special point of understanding its clients and provides experts with real world experience to work with them. CSC is vendor independent, delivering solutions that best meet each client's unique requirements.

For 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."