

## **As finance roils, don't neglect information security!!**

By Kevin M Nixon, MSA, CISSP, CISM, and Laura Wilson, JD, CISA candidate

**September 24, 2008**

While the world eyes the valuation meltdown in financial services, don't neglect the danger to regulated systems and data. The pitfalls of underestimating the financial risk of transactions are now apparent; the fallout from underestimating the information security implications of transactions is waiting in the wings. We believe that, in addition to the obvious threat to market stability, the current situation has the added element of national and global security concerns. Misuse of financial systems and information can cause widespread, immediate, and long-lasting disruption to our daily lives and our society.

It is frequently assumed that established financial services firms have the information security threat well-covered. That assumption is frequently wrong. Despite spending hundreds of millions to attempt to manage risk, significant gaps remain in the due diligence and ongoing monitoring of the business relationships that give third parties access to financial systems and data. We have encountered multiple projects involving vendors providing products and services to financial services companies, thereby having access to the Fort Knox of financial systems and accounts, and the data elements allowing entry to those accounts; however, many of the security protections, reviews, and controls that were supposed to be in place for vendors with this level of data access were bypassed. And this was during the good times.

Everybody has gaps - that's why there are internal audit and other control functions. This is not the time for finger-pointing; it's the time for finding and fixing the material gaps before we further lose control of this data.

Many of these gaps are readily fixable, and can be addressed efficiently without stopping business. Getting a better handle on vendor relationships (frequently called 'outsourcing' by the financial services industry) won't prevent all information security breaches, but financial services companies must know and monitor the parties that access information assets.

The financial services industry is well versed in the multiple laws and regulations to which it is subject. The industry consortium BITS ([www.bitsinfo.org](http://www.bitsinfo.org)) has long articulated the risks of outsourcing. Many companies have well-documented policies to address this risk. What they frequently miss is how the gaps occur, and how to fix them.

Many of the gaps happen in the contracting process - the entire lifecycle of selecting, reaching agreement with, and performing the relationship with a vendor of a product or service. The current threat environment, which includes terrorism, organized theft of individual and corporate financial assets, and just-for-fun hackers, makes new security, due diligence, and risk management demands of financial services companies. The old way of analyzing and managing these deals and business relationships cannot keep up. Because many different teams are involved in the lifecycle of a deal, because the teams have different vocabularies, areas of expertise, requirements and agendas, and because the teams find it difficult to coordinate these competing needs, the controls that are supposed to protect systems and information are often bypassed if the myriad teams do not understand the risk and how readily it can be addressed.

For a long time, the deal management function was based on a manufacturing, assembly-line model. This approach, and the compensation of the deal team, emphasized speed of the process, cost-cutting, and keeping the internal project sponsors happy ('customer satisfaction'), rather than the due diligence and control functions required for a threat environment. The deal team had little incentive to push back on an unacceptable proposal, and much of the due diligence and risk mitigation was pushed to the back end, after the deal was done and the contract signed. That's

like agreeing to pay for an expensive piece of real estate that will process sensitive radioactive material, but not inspecting the property until after the contract is signed and the check cashed.

Most business teams don't want to do the wrong thing, but many have not been given the information or tools to adequately understand the situation and make supportable decisions. Most contract and deal teams don't want to do the wrong thing, but the old job functions have not been given the gravitas, training, or compensation structure to push back on proposals that carry unacceptable risk.

It's hard enough to protect this stuff during good times. With layoffs, cost-cutting, companies folding, projects changing hands, and unhappy workers bearing flash drives, keeping track of these information assets and who touches them is a huge challenge.

This is not the time for financial services to cheap out on information security. While the industry, regulators, and consumers are watching the dollar valuation, do not forget to protect the systems and data.

Kevin M Nixon, MSA, CISSP, CISM  
Laura Wilson, JD, CISA candidate

The writers are business consultants with experience in deal analysis and information security for international financial services. They have governmental experience in handling classified information.

Copyright © - 2008. All Rights Reserved

(The writers give permission to link to, post, distribute, or reference the above article for any lawful purpose, provided that attribution is provided to the writers. This article will also be posted at the writers' own sites.)

*More to come...*

*Control bypass + information security breach = D&O liability claims, shareholder derivatives, class actions, regulatory investigations, no insurance coverage, personal liability. And more.*

*How to fix this weak link, quick.*

*Protecting your information during the storm.*

## ABOUT THE WRITERS



[Kevin M. Nixon](#) is a Master Security Architect (MSA); Certified Information Systems Security Professional (CISSP); Certified Information Security Manager (CISM); Certified US Domestic and International Regulatory Professional; and Licensed Private Security Consultant. Kevin has over 25 years of experience in MIS design and development, Information Security, Business Continuity and Disaster Recovery, and US and European Regulatory Compliance.

He testified as an expert witness before the Congressional High Tech Task Force, the Chairman of the Senate Armed Services Committee, and the Chairman of the House Ways and Means Committee. He served on infrastructure security boards and committees including:

- ◆ Disaster Recovery Workgroup for the Office of Homeland Security (which developed the [National Strategy to Secure Cyberspace](#))
- ◆ Executive Board of Directors, [Internet Security Alliance](#) (ISA)
- ◆ Chairman, Best Practices Information Security Management Committee, ISA
- ◆ Executive Board Member of the [Accredited Standards Committee, X9, Inc.](#) (the not-for-profit that develops technical standards, certified by the American National Standards Institute, for the financial services industry)
- ◆ US Voting Delegate to the [International Standards Organization](#) (ISO), Financial Data Protection, Privacy and Security Standards TC68-SC2 & US TC68-SC6
- ◆ Consultant to the Federal Trade Commission (FTC), on the administration and rollout of the Fair and Accurate Credit Transactions Act of 2003 (FACTA) Web Portal, [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com)

### Other contributions include:

- ◆ Consultant to VISA in 2002 to develop the [Cardholder Information Security Program \(CISP\)](#), the basis for the [Payment Card Industry Data Security Standards \(PCI DSS\)](#)
- ◆ Co-Author of a 3-Part Series of "Common Sense Security Guides", including THE COMMON SENSE GUIDE FOR SENIOR MANAGERS - Top Ten Recommended Information Security Practices, 1st Edition - July 2002, Internet Security Alliance, which is now used by the US Department of Homeland Security, National Association of Manufacturers, American Bankers Association, The National Federation of Independent Businesses, The National Cyber Security Alliance, Financial Services Coordinating Sector, TechNet, and US-India Business Council
- ◆ [The Cyber Security Guide for Executives & Senior Managers](#)
- ◆ [The Cyber Security Guide for Small Businesses](#)
- ◆ [They Cyber Security Guide for Virtual Employees & Mobile Executives](#)
- ◆ Appeared as Cyber-terrorism Expert on CNBC's Squawk Box with Mark Haines
- ◆ Appeared as Identity Privacy Protection Expert on [KUCI Radio's Privacy Piracy with Mari Frank](#)

Kevin's business experience includes serving as the Banking Security Officer of World Financial Network National Bank. Kevin has held positions of oversight of all regulatory compliance, data security, and data privacy issues, compliance with FFIEC Banking Regulations, and direction of OCC and SAS 70 Audits for his clients.

[www.GRCandPrivacy.com](http://www.GRCandPrivacy.com)

<http://www.linkedin.com/in/kevinnixon>



**[Laura Wilson](#)** is a privacy advocate, and a business consultant working in governance / risk / compliance, deal analysis, and problem resolution related to highly sensitive systems and data.

She has over 10 years of experience in business and legal roles for highly regulated organizations, including publicly-traded international financial services (banking / payment card industry / mortgages / insurance / investment advisors), venture capital portfolio companies, and numerous software and services projects involving regulated systems and sensitive data.

The companies for which Laura has negotiated and managed complex outsourcing and vendor relationships include:

- ◆ A publicly-traded global credit card company that co-authored the PCI DSS (Payment Card Industry Data Security Standards)
- ◆ One of the largest publicly-traded mortgage companies in the U.S.
- ◆ A publicly-traded international investment advisory firm

Laura has trained colleagues on industry standards, gap analysis and risk mitigation. She writes training materials and works on dashboard design to help stakeholders identify and remedy compliance and security gaps, and verify appropriate due diligence. She volunteers with the [Phoenix chapter of ISACA](#), and other professional groups and not-for-profits interested in the regulatory, governance, information security and national security implications of financial systems and regulated data. She has been interviewed on [KUCI \(UC-Irvine\)](#), [Privacy Piracy with Mari Frank](#), regarding information security.

Laura holds a Juris Doctor, (licensed as an attorney in California), and is a CISA (Certified Information Systems Auditor) candidate (passed CISA exam; certification pending). She is pursuing additional information security certifications.

Laura served on active duty for over 8 years in the United States Army. She was a Staff Sergeant, paratrooper, and TV / radio broadcaster; served in Military Intelligence, Psychological Operations, Communications, and Public Relations positions; and won several Soldier of the Year awards.

[www.techlex.com](http://www.techlex.com)

<http://www.linkedin.com/in/lwilsontech>

# # #